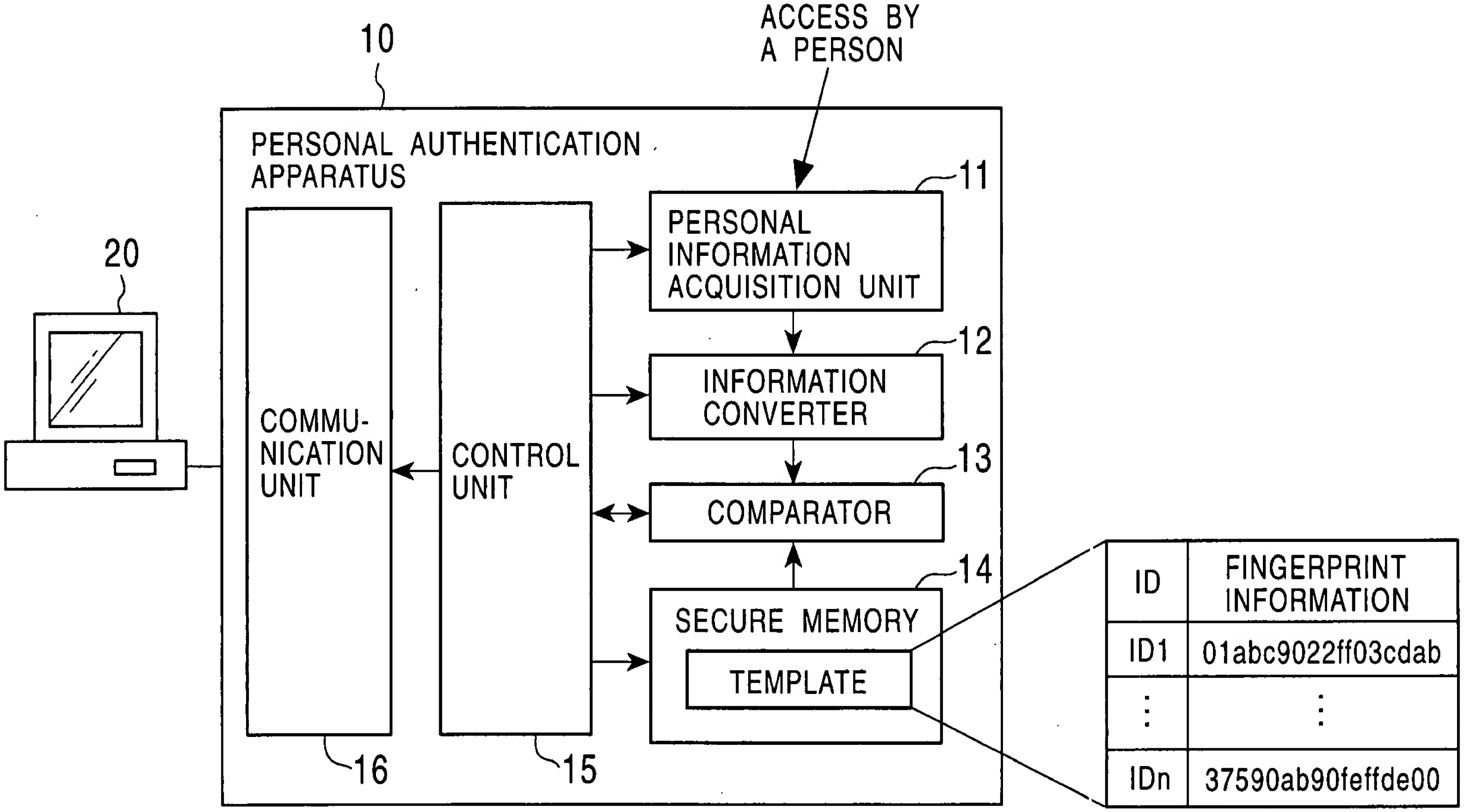
S01P1294

FIG. 1



ID	FINGERPRINT INFORMATION
ID1	01abc9022ff03cdab
⋮	⋮
IDn	37590ab90feffde00

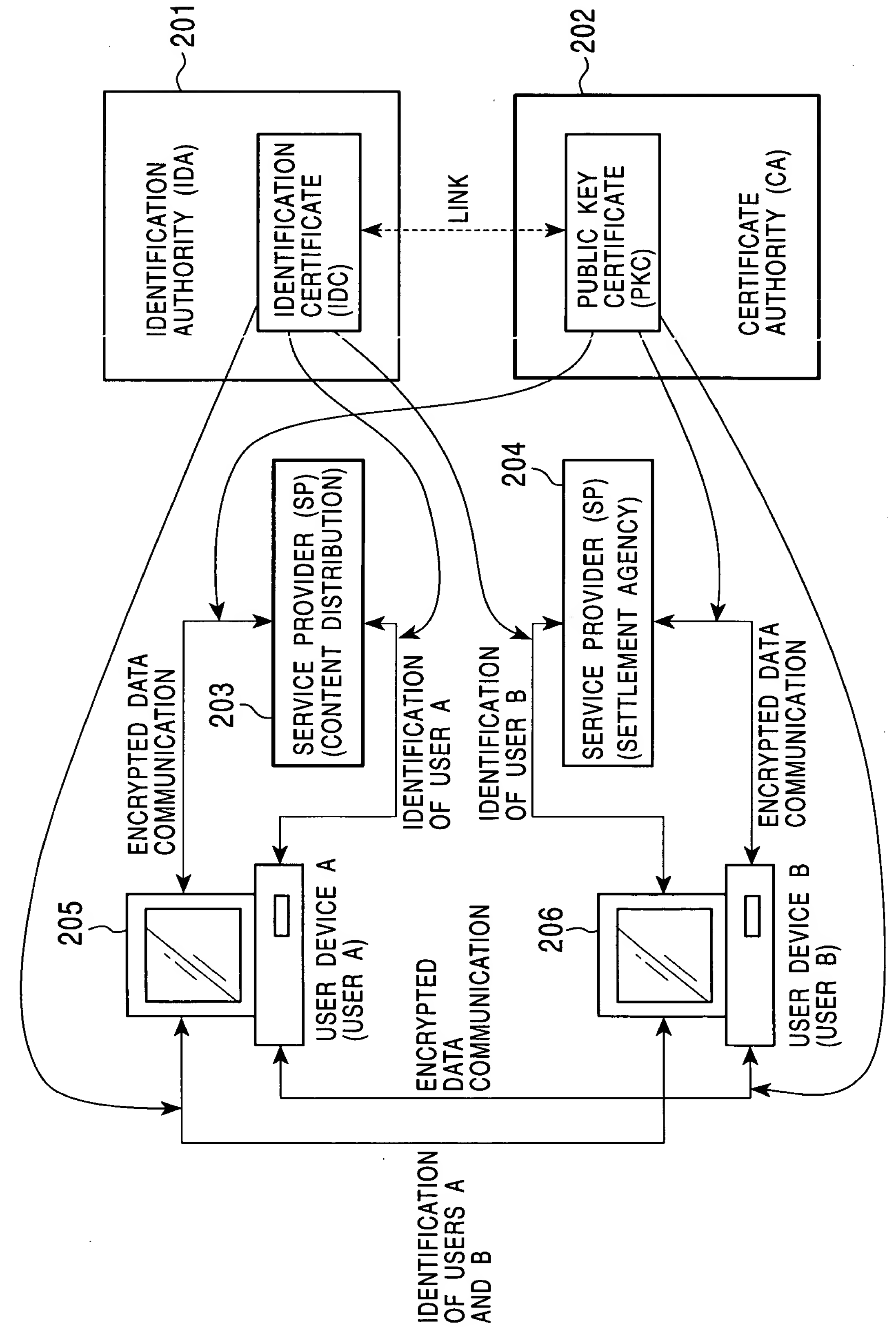

201
IDENTIFICATION AUTHORITY (IDA)
IDENTIFICATION CERTIFICATE (IDC)
LINK
202
PUBLIC KEY CERTIFICATE (PKC)
CERTIFICATE AUTHORITY (CA)
203
SERVICE PROVIDER (SP) (CONTENT DISTRIBUTION)
204
SERVICE PROVIDER (SP) (SETTLEMENT AGENCY)
ENCRYPTED DATA COMMUNICATION
IDENTIFICATION OF USER A
IDENTIFICATION OF USER B
ENCRYPTED DATA COMMUNICATION
205
USER DEVICE A (USER A)
206
USER DEVICE B (USER B)
ENCRYPTED DATA COMMUNICATION
IDENTIFICATION OF USERS A AND B

FIG. 2

FIG. 3

Item	Description	Value employed in the present IA
Version 1		
version	Version of the certificate format	V3
serial Number	Serial number of the certificate assigned by the IA	Assigned in a serial fashion
signature algorithm Identifier algorithm parameters	Algorithm of the signature of the certificate and parameters thereof	Elliptic curve number/RSA parameters when an elliptic curve is used Key length when RSA is employed
issuer	IA name (in a distiguished name form)	Name of the present IA
validity notBefore notAfter	Period during which the certificate is valid Start date Expiration date	
subject	Name which identifies the user	User device ID or ID of the service subject
subject Public Key Info algorithm subject Public key	Information of the public key of the user Algorithem of the key Key	 Elliptic curve/RSA Public key of the user
Version 3		
authority Key Identifier key Identifier authority Cert Issuer authority Cert Serial Number	Key identifier used in verification of the IA Key identification number (octal number) Name of the IA (in a general name form) Identification number	
subject key Identifier	Used when a plurality of keys are certified	Not used
key usage (0)digital Signature (1)non Repudiation (2)key Encipherment (3)data Encipherment (4)key Agreement (5)key CertSign (6)cRL Sign	Specifying the purpose of the key (0)for digital signature (1)to prevent repudiation (2)for encryption of the Key (3)for encryption of a message (4)for use in transmission of a symmetric key (5)used to verify the certificate (6)used to verify the signature of the certificate revolution list	0,1,4, or 6 is used
private Key Usage Period notBefore notAfter	Period during which the private key stored in the user is valid	Usage period is the same for the certificate, the public key, and the private Key (default)

FIG. 4

Certificate Policy policy Identifier policy Qualifers	Certificate policy of the certificate authority Policy ID (according to ISO/IEC9834-1) Certification criteria	
policy Mappings issuer Domain Policy subject Domain Policy	Required only when the CA is certificated. Mappings of the policy of the issuer domain policy and the subject domain policy are defined	default = none
supported Algorithms algorithm Identifier intended Usage intended Certificate Policies	Attributes of the directory (X.500) are defined. Used to inform a receiving party of communication of the attributes the direction so that the receiving party can use the direction information	default = none
subject Alt Name	Alternative name of the user (in the form of GN)	not used
issuer Alt Name	Not used although this item is included in the certificate format (default = none)	default = none
subject Directory Attributes	Arbitrary attributes of the user	not used
basic Constraints	Specifies the public key to be certified	
cA path Len Constraint	Indicates whether the public key is used by a user or by a certificate authority to write a signature	default = used by a user
name Constraints permitted Subtrees base minimum	Used only when the certification is to certify a certification authority (CA)	default = none
maximum excluded Subtrees		
policy Constraints requier Explicit Policy inhibit Policy Mapping	Constraints are described in terms of requirements of explicit policy ID or inhibit policy mapping for the remaining certification path	
CRL Distribution Points	Indicates a reference point in the revocation list at which data is present which indicates whether the certificate of a user is revocated	Pointer which points to a location where the certificate is registered. The revocation list is managed by an issuer
Signature	Signature of the issuer	

FIG. 5

	Item	Description
Indis-pensable Items	Version	Version
	Serial Number	Identification Number
	signature algorithm Identifier algorithm parameters	Signature algorithem Algorithm Parameters
	Issuer	Name of the identification authority (in the form of a distinguished name)
	Validity notBefore notAfter	Period during which the certificate is valid Start date Expiration date
	Subject	Name of the subject to be certificated (in a DN form)
Extended Items	subject Template Info encrypt Type encrypt Unique ID encryption Algorithm parameter validity subject Template Source subject Template	Template information • encrypt Type • The unique ID or the certificate number of a public key certificate used for encryption • Algorithm • parameter • Validity period (start date, expiration date) • Type of the template • Template
	Subject PKC info subject PKC serial Number subject PKC Unique ID	Information about the public key certificate of the subject • Certificate number of the subject public key certificate • Unique ID of the subject of the subject public key certificate
	Issuer Unique ID	Unique ID of the issuer
	Subject Unique ID	Unique ID of the subject
	Public Key Certificate	Public key certificate
	Issuer Alt Name	Alternative name of the issuer
	subject Directory Attributes	Personal information (encrypted as required) information used to authenticate subject Age, sex, etc.
	Valid Count	Number of times the certificate is allowed to be used
	Control Table Link Info Ctl Tbl Location Ctl Tbl Unique ID	Link information describing group information • Location of a link information control table (URL, IP address, etc.) • Identification number of the link information
Indispen-sable	IDA Signature	Signature of the IDA

FIG. 6A

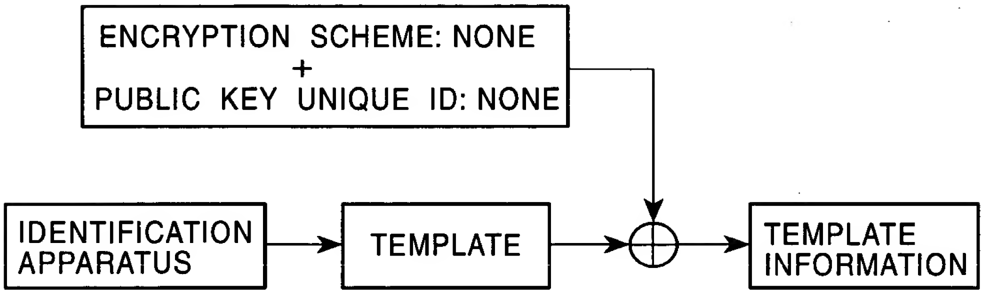


FIG. 6B

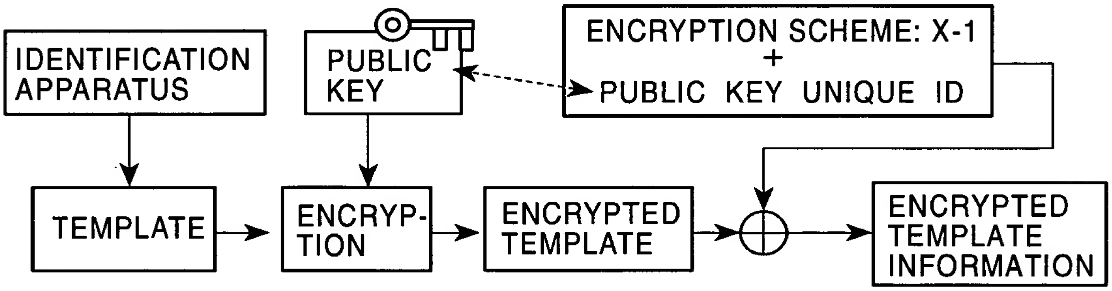


FIG. 6C

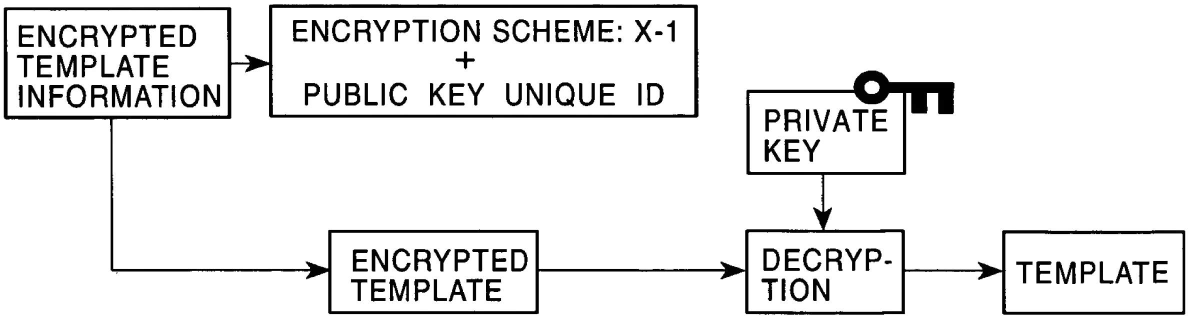


FIG. 7

PUBLIC KEY USED TO ENCRYPT TEMPLATES	EXAMPLES OF MANNERS IN WHICH TEMPLATE INFORMATION STORAGE IDC IS USED
PUBLEC KEY OF A USER OR A USER DEVICE	TO IDENTIFY AN AUTHORIZED USER OF A USER DEVICE (SUCH AS A PC) ON THE BASIS OF AN IDENTIFICATION CERTIFICATE OF THE USER
PUBLIC KEY OF A SERVICE PROVIDER	USED BY A SERVICE PROVIDER TO IDENTIFY A PARTICULAR USER SUCH AS A USER TO WHOM SERVICE IS TO BE PROVIDED, ON THE BASIS OF AN IDENTIFICATION CERTIFICATE (IDC) OF THE USER
PUBLIC KEY OF AN IDENTIFICATION AUTHORITY	IN DATA TRANSMISSION AMONG VARIOUS TERMINALS, A SENDER OR A RECEIVER IDENTIFIES

FIG. 8A

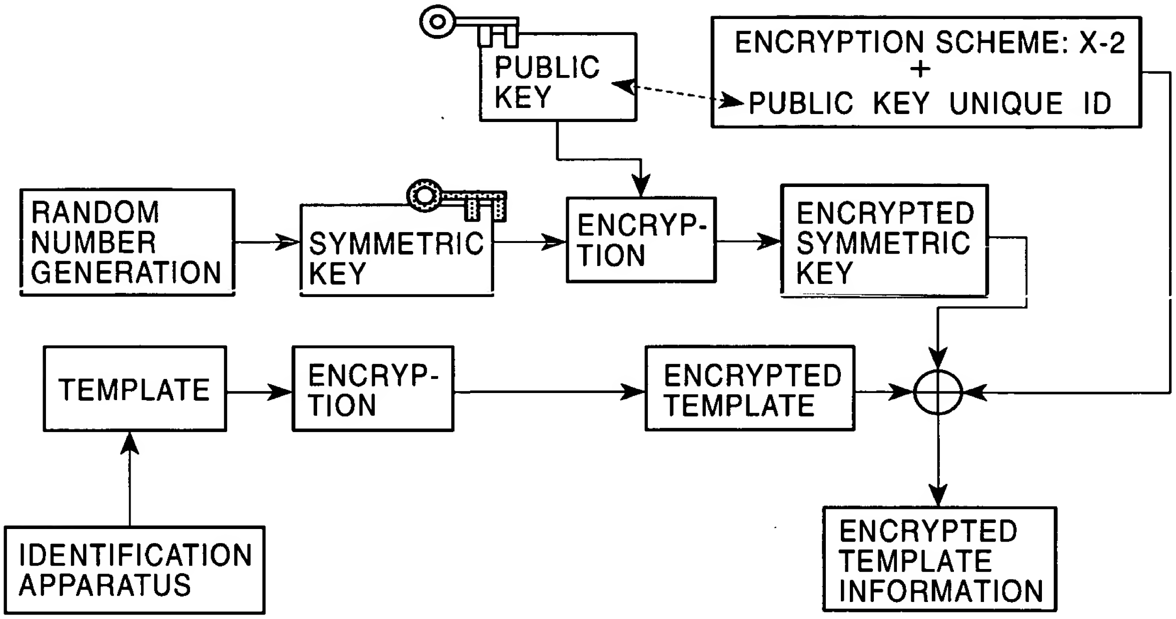

PUBLIC KEY
ENCRYPTION SCHEME: X-2 + PUBLIC KEY UNIQUE ID
RANDOM NUMBER GENERATION
SYMMETRIC KEY
ENCRYP-TION
ENCRYPTED SYMMETRIC KEY
TEMPLATE
ENCRYP-TION
ENCRYPTED TEMPLATE
IDENTIFICATION APPARATUS
ENCRYPTED TEMPLATE INFORMATION

FIG. 8B

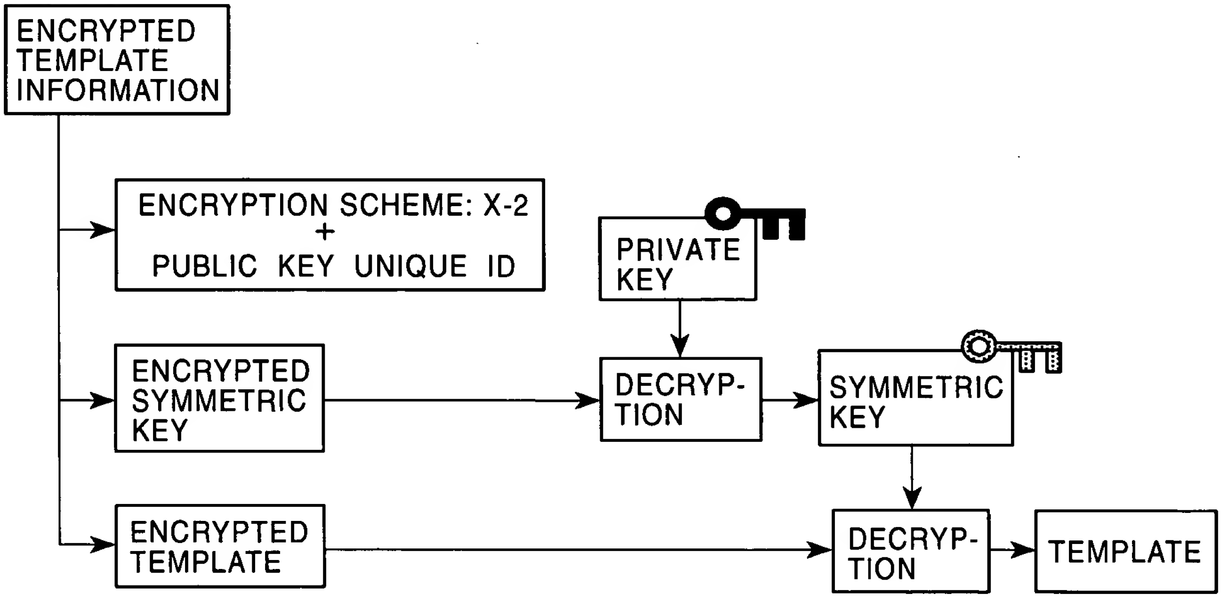

ENCRYPTED TEMPLATE INFORMATION
ENCRYPTION SCHEME: X-2 + PUBLIC KEY UNIQUE ID
PRIVATE KEY
ENCRYPTED SYMMETRIC KEY
DECRYP-TION
SYMMETRIC KEY
ENCRYPTED TEMPLATE
DECRYP-TION
TEMPLATE

FIG. 9

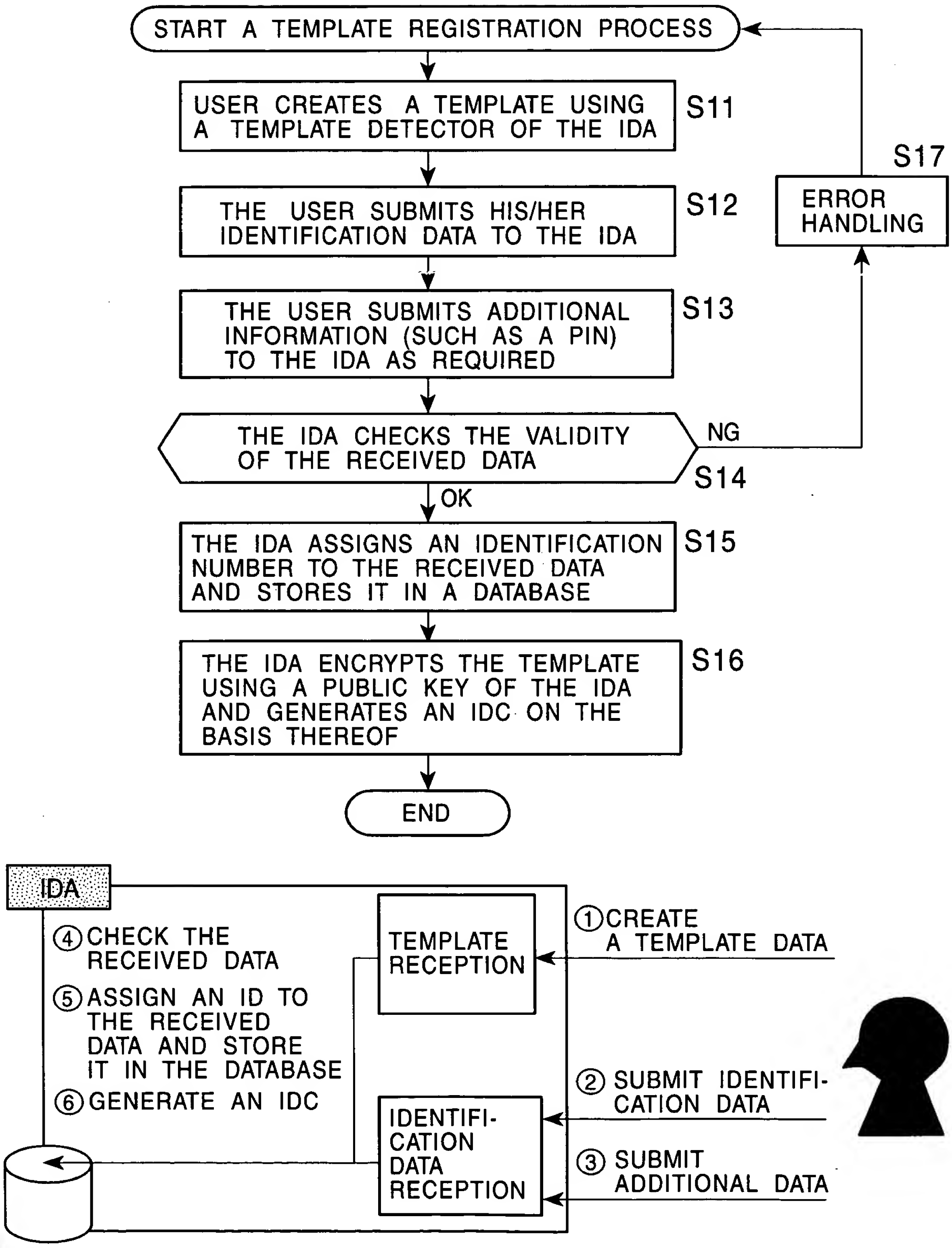

START A TEMPLATE REGISTRATION PROCESS
USER CREATES A TEMPLATE USING A TEMPLATE DETECTOR OF THE IDA
S11
THE USER SUBMITS HIS/HER IDENTIFICATION DATA TO THE IDA
S12
THE USER SUBMITS ADDITIONAL INFORMATION (SUCH AS A PIN) TO THE IDA AS REQUIRED
S13
THE IDA CHECKS THE VALIDITY OF THE RECEIVED DATA
S14
NG
OK
ERROR HANDLING
S17
THE IDA ASSIGNS AN IDENTIFICATION NUMBER TO THE RECEIVED DATA AND STORES IT IN A DATABASE
S15
THE IDA ENCRYPTS THE TEMPLATE USING A PUBLIC KEY OF THE IDA AND GENERATES AN IDC ON THE BASIS THEREOF
S16
END
IDA
④ CHECK THE RECEIVED DATA
⑤ ASSIGN AN ID TO THE RECEIVED DATA AND STORE IT IN THE DATABASE
⑥ GENERATE AN IDC
TEMPLATE RECEPTION
IDENTIFICATION DATA RECEPTION
① CREATE A TEMPLATE DATA
② SUBMIT IDENTIFICATION DATA
③ SUBMIT ADDITIONAL DATA

FIG. 10

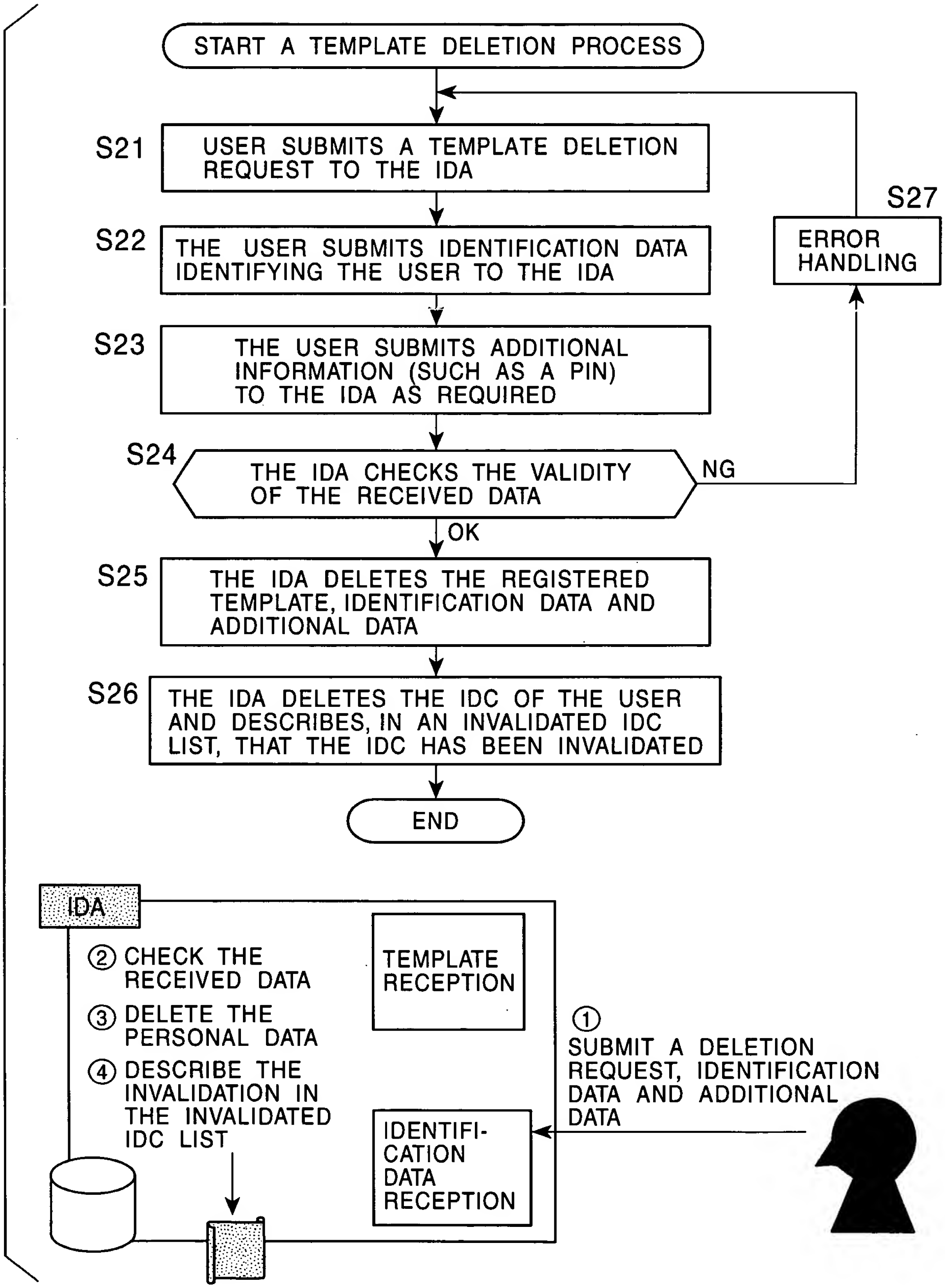

START A TEMPLATE DELETION PROCESS
S21
USER SUBMITS A TEMPLATE DELETION REQUEST TO THE IDA
S22
THE USER SUBMITS IDENTIFICATION DATA IDENTIFYING THE USER TO THE IDA
S23
THE USER SUBMITS ADDITIONAL INFORMATION (SUCH AS A PIN) TO THE IDA AS REQUIRED
S24
THE IDA CHECKS THE VALIDITY OF THE RECEIVED DATA
NG
S27
ERROR HANDLING
OK
S25
THE IDA DELETES THE REGISTERED TEMPLATE, IDENTIFICATION DATA AND ADDITIONAL DATA
S26
THE IDA DELETES THE IDC OF THE USER AND DESCRIBES, IN AN INVALIDATED IDC LIST, THAT THE IDC HAS BEEN INVALIDATED
END
IDA
② CHECK THE RECEIVED DATA
③ DELETE THE PERSONAL DATA
④ DESCRIBE THE INVALIDATION IN THE INVALIDATED IDC LIST
TEMPLATE RECEPTION
IDENTIFI-CATION DATA RECEPTION
① SUBMIT A DELETION REQUEST, IDENTIFICATION DATA AND ADDITIONAL DATA

FIG. 11

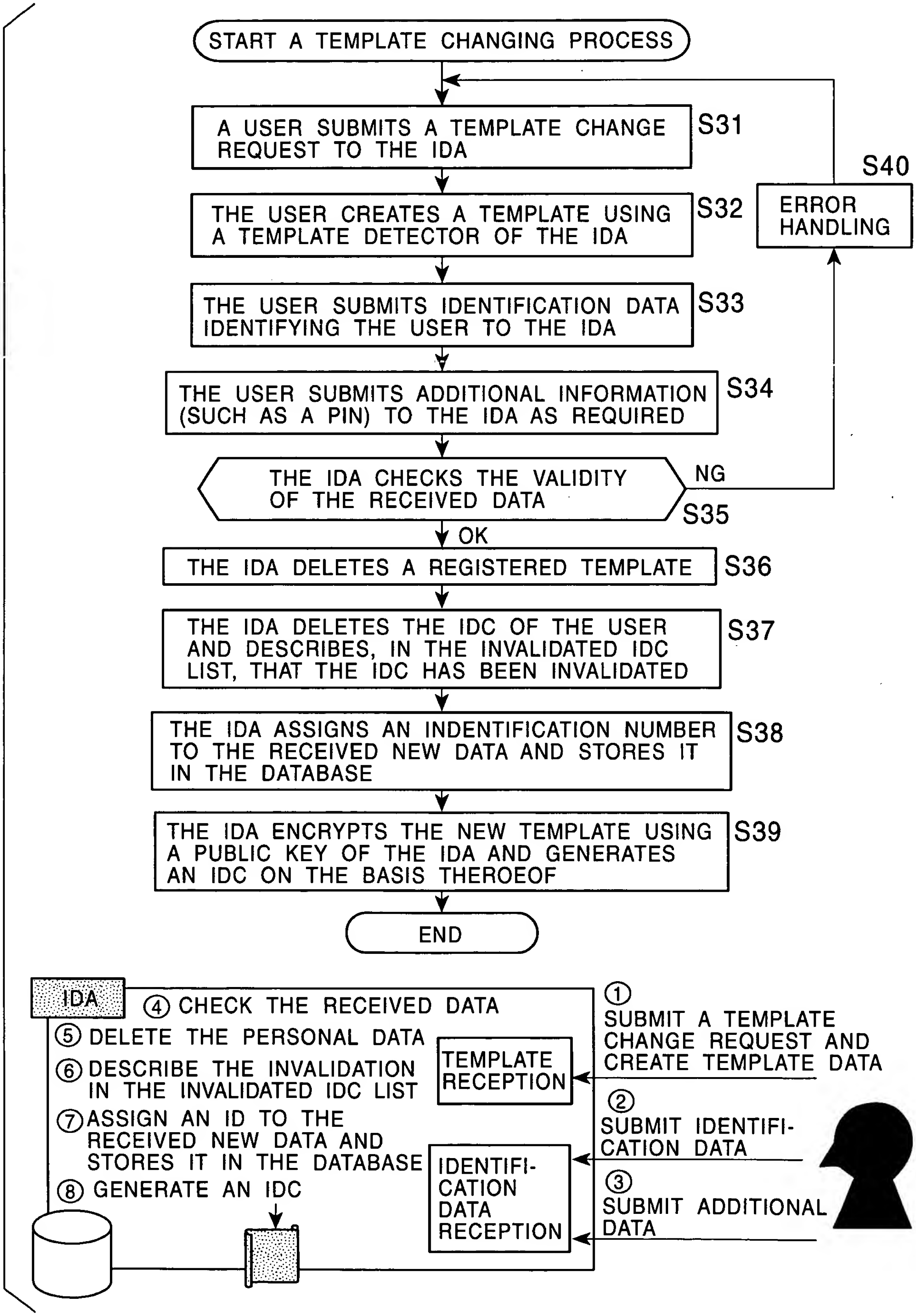

START A TEMPLATE CHANGING PROCESS
A USER SUBMITS A TEMPLATE CHANGE REQUEST TO THE IDA
S31
THE USER CREATES A TEMPLATE USING A TEMPLATE DETECTOR OF THE IDA
S32
THE USER SUBMITS IDENTIFICATION DATA IDENTIFYING THE USER TO THE IDA
S33
THE USER SUBMITS ADDITIONAL INFORMATION (SUCH AS A PIN) TO THE IDA AS REQUIRED
S34
THE IDA CHECKS THE VALIDITY OF THE RECEIVED DATA
S35
NG
OK
S40
ERROR HANDLING
THE IDA DELETES A REGISTERED TEMPLATE
S36
THE IDA DELETES THE IDC OF THE USER AND DESCRIBES, IN THE INVALIDATED IDC LIST, THAT THE IDC HAS BEEN INVALIDATED
S37
THE IDA ASSIGNS AN INDENTIFICATION NUMBER TO THE RECEIVED NEW DATA AND STORES IT IN THE DATABASE
S38
THE IDA ENCRYPTS THE NEW TEMPLATE USING A PUBLIC KEY OF THE IDA AND GENERATES AN IDC ON THE BASIS THEROEOF
S39
END
IDA
④ CHECK THE RECEIVED DATA
⑤ DELETE THE PERSONAL DATA
⑥ DESCRIBE THE INVALIDATION IN THE INVALIDATED IDC LIST
⑦ ASSIGN AN ID TO THE RECEIVED NEW DATA AND STORES IT IN THE DATABASE
⑧ GENERATE AN IDC
TEMPLATE RECEPTION
IDENTIFI-CATION DATA RECEPTION
① SUBMIT A TEMPLATE CHANGE REQUEST AND CREATE TEMPLATE DATA
② SUBMIT IDENTIFI-CATION DATA
③ SUBMIT ADDITIONAL DATA

FIG. 12

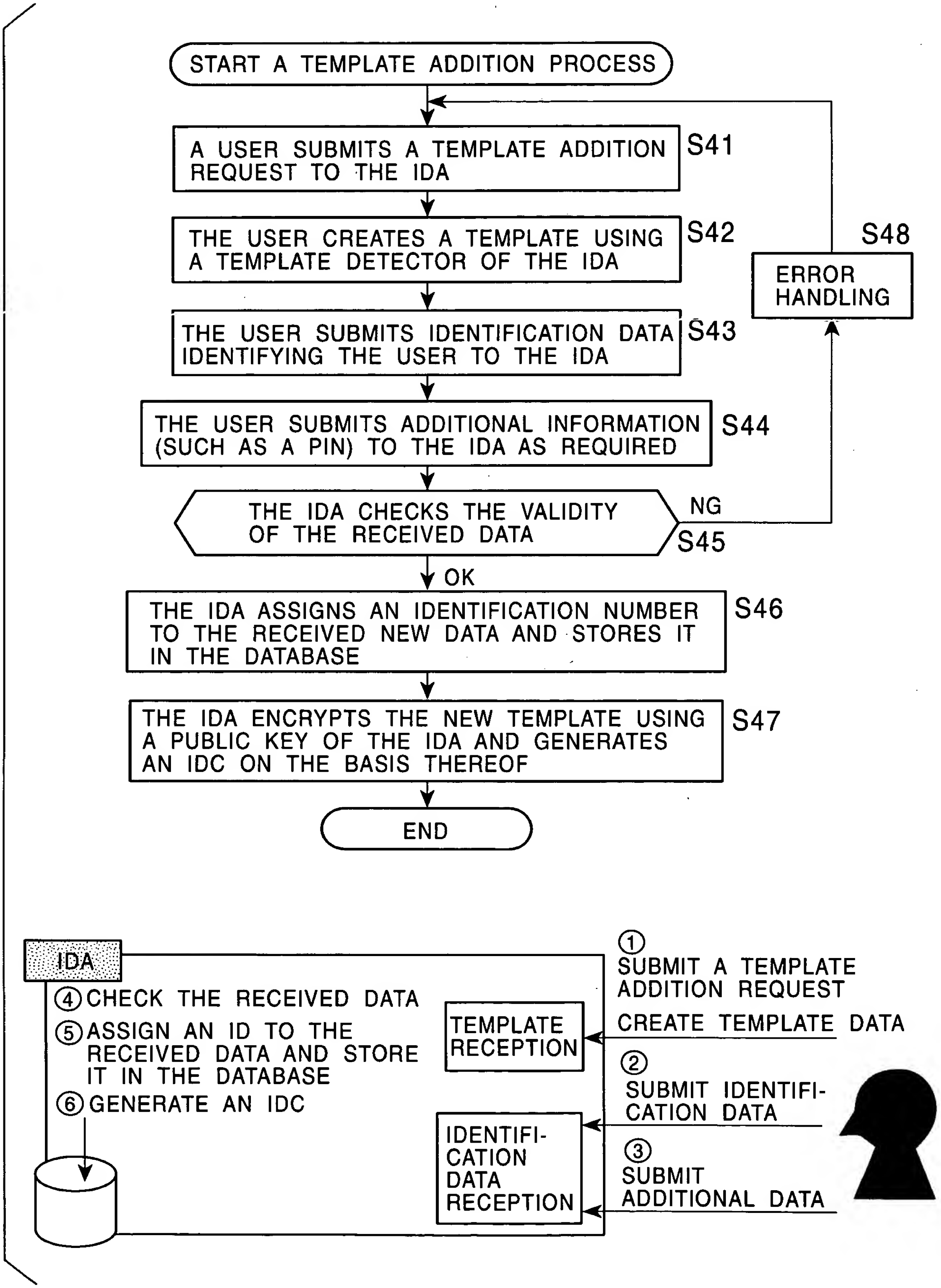

START A TEMPLATE ADDITION PROCESS
A USER SUBMITS A TEMPLATE ADDITION REQUEST TO THE IDA
S41
THE USER CREATES A TEMPLATE USING A TEMPLATE DETECTOR OF THE IDA
S42
THE USER SUBMITS IDENTIFICATION DATA IDENTIFYING THE USER TO THE IDA
S43
THE USER SUBMITS ADDITIONAL INFORMATION (SUCH AS A PIN) TO THE IDA AS REQUIRED
S44
THE IDA CHECKS THE VALIDITY OF THE RECEIVED DATA
S45
NG
S48
ERROR HANDLING
OK
THE IDA ASSIGNS AN IDENTIFICATION NUMBER TO THE RECEIVED NEW DATA AND STORES IT IN THE DATABASE
S46
THE IDA ENCRYPTS THE NEW TEMPLATE USING A PUBLIC KEY OF THE IDA AND GENERATES AN IDC ON THE BASIS THEREOF
S47
END
IDA
④CHECK THE RECEIVED DATA
⑤ASSIGN AN ID TO THE RECEIVED DATA AND STORE IT IN THE DATABASE
⑥GENERATE AN IDC
TEMPLATE RECEPTION
IDENTIFICATION DATA RECEPTION
① SUBMIT A TEMPLATE ADDITION REQUEST
CREATE TEMPLATE DATA
② SUBMIT IDENTIFICATION DATA
③ SUBMIT ADDITIONAL DATA

FIG. 13

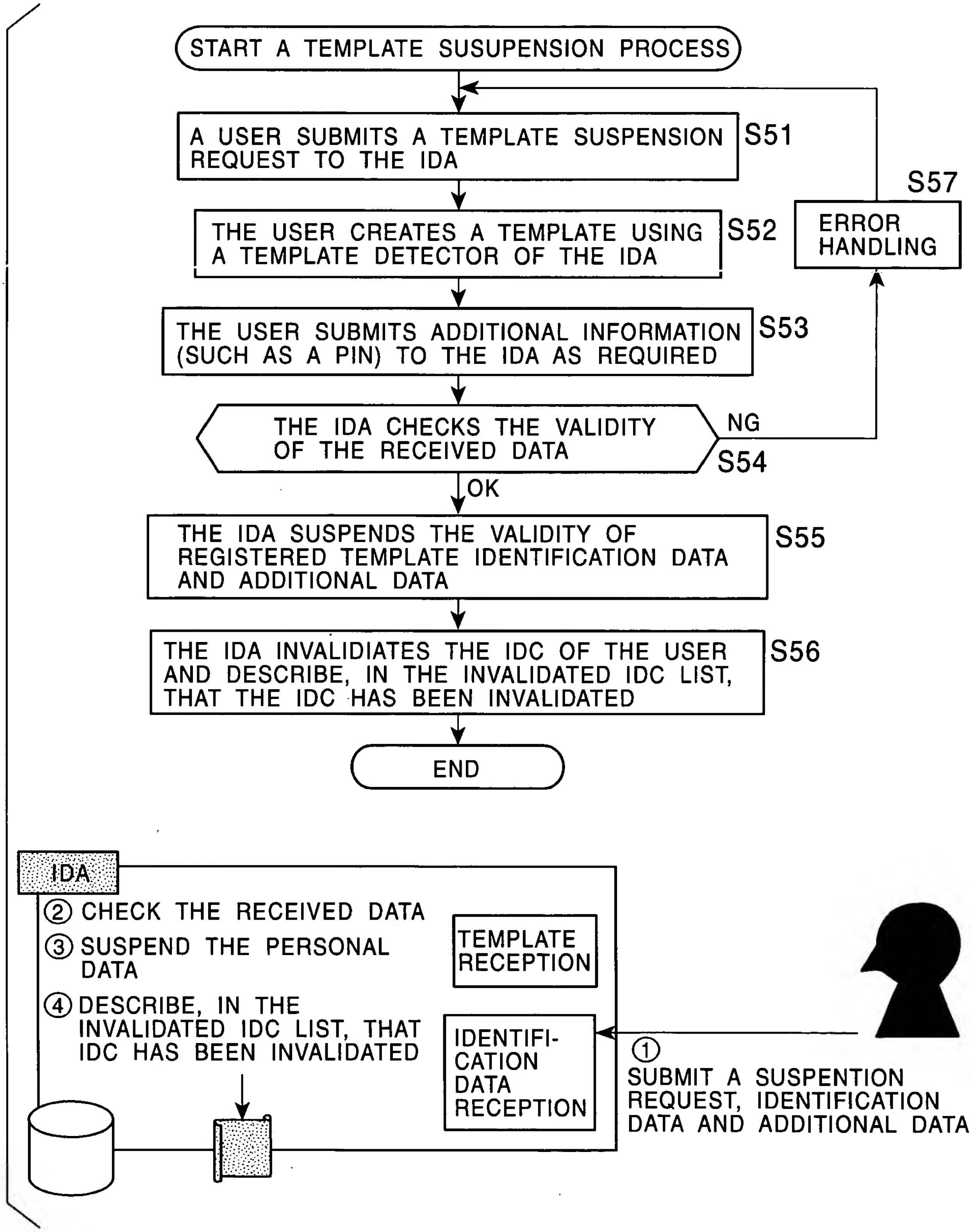

START A TEMPLATE SUSUPENSION PROCESS
A USER SUBMITS A TEMPLATE SUSPENSION REQUEST TO THE IDA
S51
THE USER CREATES A TEMPLATE USING A TEMPLATE DETECTOR OF THE IDA
S52
THE USER SUBMITS ADDITIONAL INFORMATION (SUCH AS A PIN) TO THE IDA AS REQUIRED
S53
THE IDA CHECKS THE VALIDITY OF THE RECEIVED DATA
S54
NG
OK
S57
ERROR HANDLING
THE IDA SUSPENDS THE VALIDITY OF REGISTERED TEMPLATE IDENTIFICATION DATA AND ADDITIONAL DATA
S55
THE IDA INVALIDIATES THE IDC OF THE USER AND DESCRIBE, IN THE INVALIDATED IDC LIST, THAT THE IDC HAS BEEN INVALIDATED
S56
END
IDA
② CHECK THE RECEIVED DATA
③ SUSPEND THE PERSONAL DATA
④ DESCRIBE, IN THE INVALIDATED IDC LIST, THAT IDC HAS BEEN INVALIDATED
TEMPLATE RECEPTION
IDENTIFI-CATION DATA RECEPTION
① SUBMIT A SUSPENTION REQUEST, IDENTIFICATION DATA AND ADDITIONAL DATA

FIG. 14

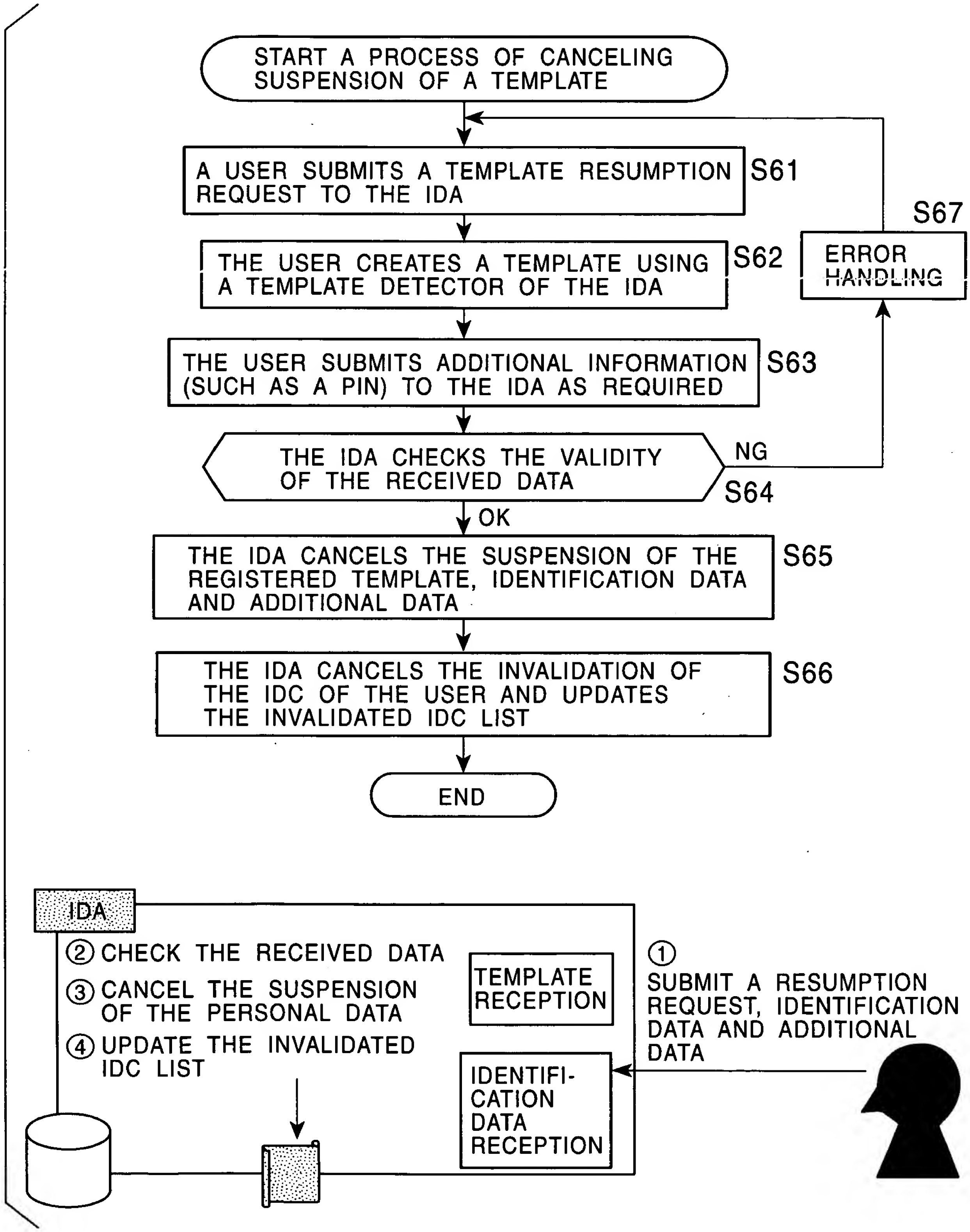

START A PROCESS OF CANCELING SUSPENSION OF A TEMPLATE
A USER SUBMITS A TEMPLATE RESUMPTION REQUEST TO THE IDA
S61
THE USER CREATES A TEMPLATE USING A TEMPLATE DETECTOR OF THE IDA
S62
THE USER SUBMITS ADDITIONAL INFORMATION (SUCH AS A PIN) TO THE IDA AS REQUIRED
S63
THE IDA CHECKS THE VALIDITY OF THE RECEIVED DATA
S64
NG
S67
ERROR HANDLING
OK
THE IDA CANCELS THE SUSPENSION OF THE REGISTERED TEMPLATE, IDENTIFICATION DATA AND ADDITIONAL DATA
S65
THE IDA CANCELS THE INVALIDATION OF THE IDC OF THE USER AND UPDATES THE INVALIDATED IDC LIST
S66
END
IDA
② CHECK THE RECEIVED DATA
③ CANCEL THE SUSPENSION OF THE PERSONAL DATA
④ UPDATE THE INVALIDATED IDC LIST
TEMPLATE RECEPTION
IDENTIFI-CATION DATA RECEPTION
①
SUBMIT A RESUMPTION REQUEST, IDENTIFICATION DATA AND ADDITIONAL DATA

FIG. 15

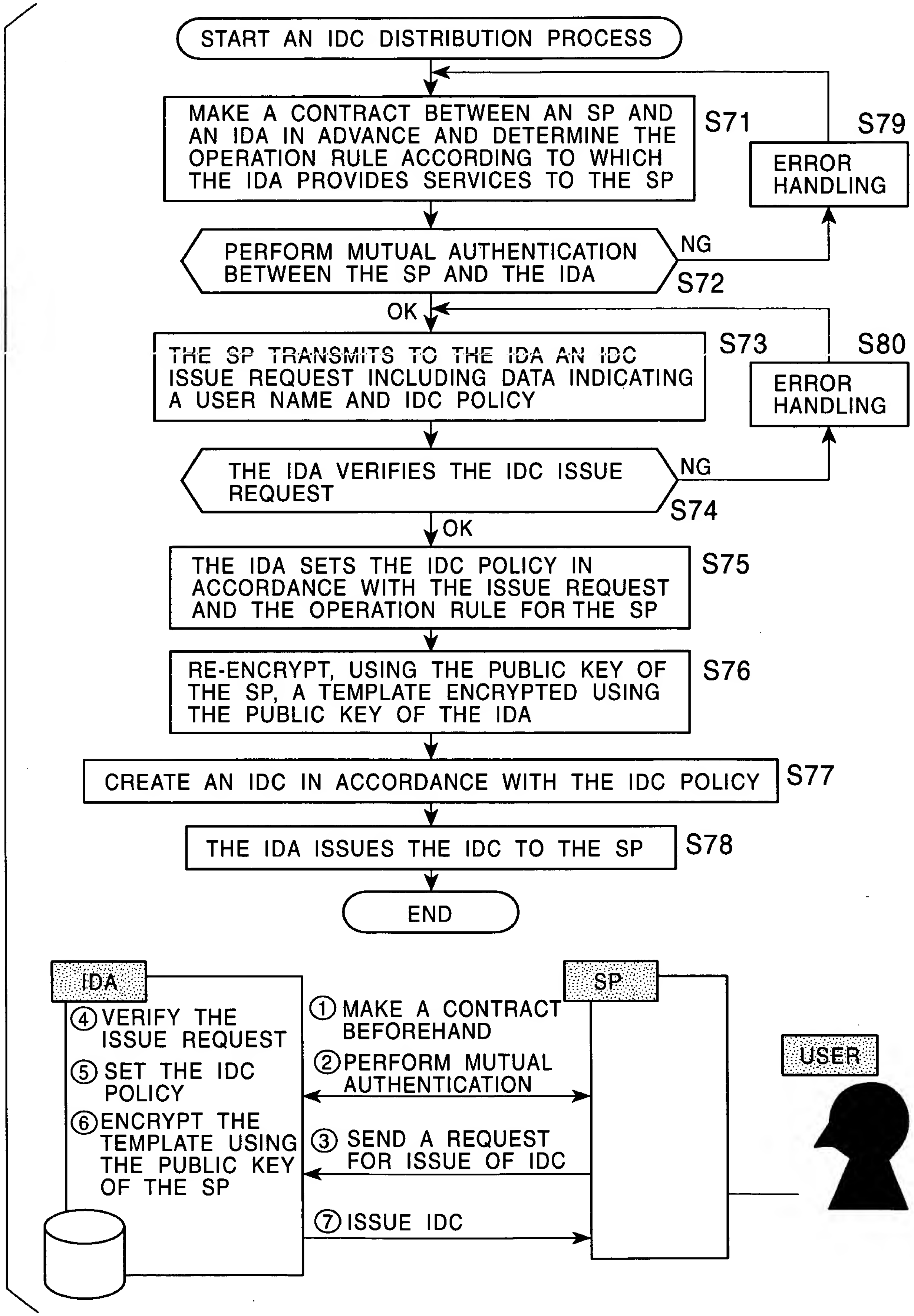

START AN IDC DISTRIBUTION PROCESS
MAKE A CONTRACT BETWEEN AN SP AND AN IDA IN ADVANCE AND DETERMINE THE OPERATION RULE ACCORDING TO WHICH THE IDA PROVIDES SERVICES TO THE SP
S71
S79
ERROR HANDLING
PERFORM MUTUAL AUTHENTICATION BETWEEN THE SP AND THE IDA
NG
S72
OK
THE SP TRANSMITS TO THE IDA AN IDC ISSUE REQUEST INCLUDING DATA INDICATING A USER NAME AND IDC POLICY
S73
S80
ERROR HANDLING
THE IDA VERIFIES THE IDC ISSUE REQUEST
NG
S74
OK
THE IDA SETS THE IDC POLICY IN ACCORDANCE WITH THE ISSUE REQUEST AND THE OPERATION RULE FOR THE SP
S75
RE-ENCRYPT, USING THE PUBLIC KEY OF THE SP, A TEMPLATE ENCRYPTED USING THE PUBLIC KEY OF THE IDA
S76
CREATE AN IDC IN ACCORDANCE WITH THE IDC POLICY
S77
THE IDA ISSUES THE IDC TO THE SP
S78
END
IDA
④VERIFY THE ISSUE REQUEST
⑤SET THE IDC POLICY
⑥ENCRYPT THE TEMPLATE USING THE PUBLIC KEY OF THE SP
①MAKE A CONTRACT BEFOREHAND
②PERFORM MUTUAL AUTHENTICATION
③SEND A REQUEST FOR ISSUE OF IDC
⑦ISSUE IDC
SP
USER

FIG. 16

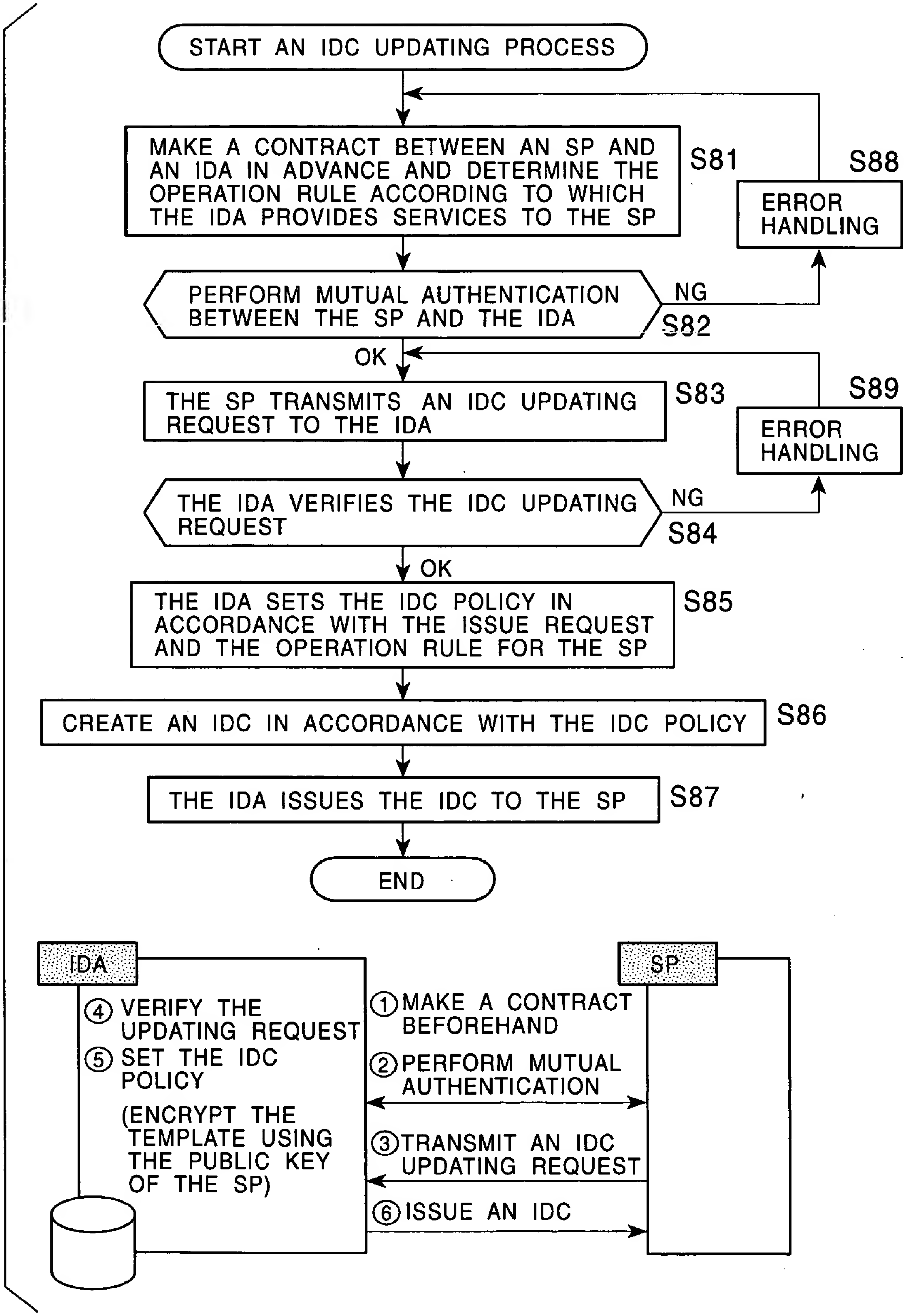

START AN IDC UPDATING PROCESS
MAKE A CONTRACT BETWEEN AN SP AND AN IDA IN ADVANCE AND DETERMINE THE OPERATION RULE ACCORDING TO WHICH THE IDA PROVIDES SERVICES TO THE SP
S81
S88
ERROR HANDLING
PERFORM MUTUAL AUTHENTICATION BETWEEN THE SP AND THE IDA
NG
S82
OK
THE SP TRANSMITS AN IDC UPDATING REQUEST TO THE IDA
S83
S89
ERROR HANDLING
THE IDA VERIFIES THE IDC UPDATING REQUEST
NG
S84
OK
THE IDA SETS THE IDC POLICY IN ACCORDANCE WITH THE ISSUE REQUEST AND THE OPERATION RULE FOR THE SP
S85
CREATE AN IDC IN ACCORDANCE WITH THE IDC POLICY
S86
THE IDA ISSUES THE IDC TO THE SP
S87
END
IDA
④ VERIFY THE UPDATING REQUEST
⑤ SET THE IDC POLICY
(ENCRYPT THE TEMPLATE USING THE PUBLIC KEY OF THE SP)
SP
① MAKE A CONTRACT BEFOREHAND
② PERFORM MUTUAL AUTHENTICATION
③ TRANSMIT AN IDC UPDATING REQUEST
⑥ ISSUE AN IDC

FIG. 17

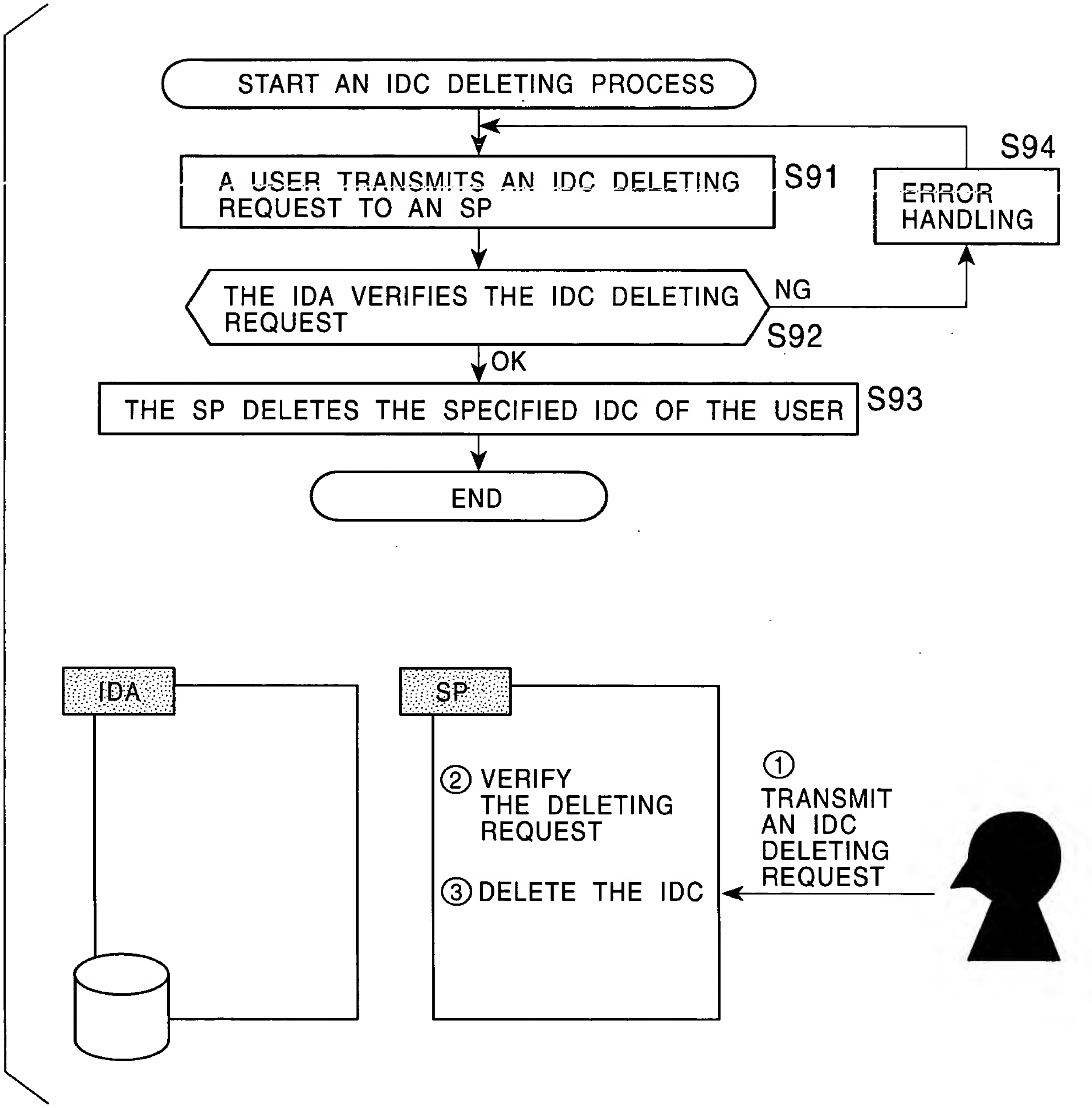

START AN IDC DELETING PROCESS
A USER TRANSMITS AN IDC DELETING REQUEST TO AN SP
S91
S94
ERROR HANDLING
THE IDA VERIFIES THE IDC DELETING REQUEST
NG
S92
OK
THE SP DELETES THE SPECIFIED IDC OF THE USER
S93
END
IDA
SP
② VERIFY THE DELETING REQUEST
③ DELETE THE IDC
① TRANSMIT AN IDC DELETING REQUEST

FIG. 18

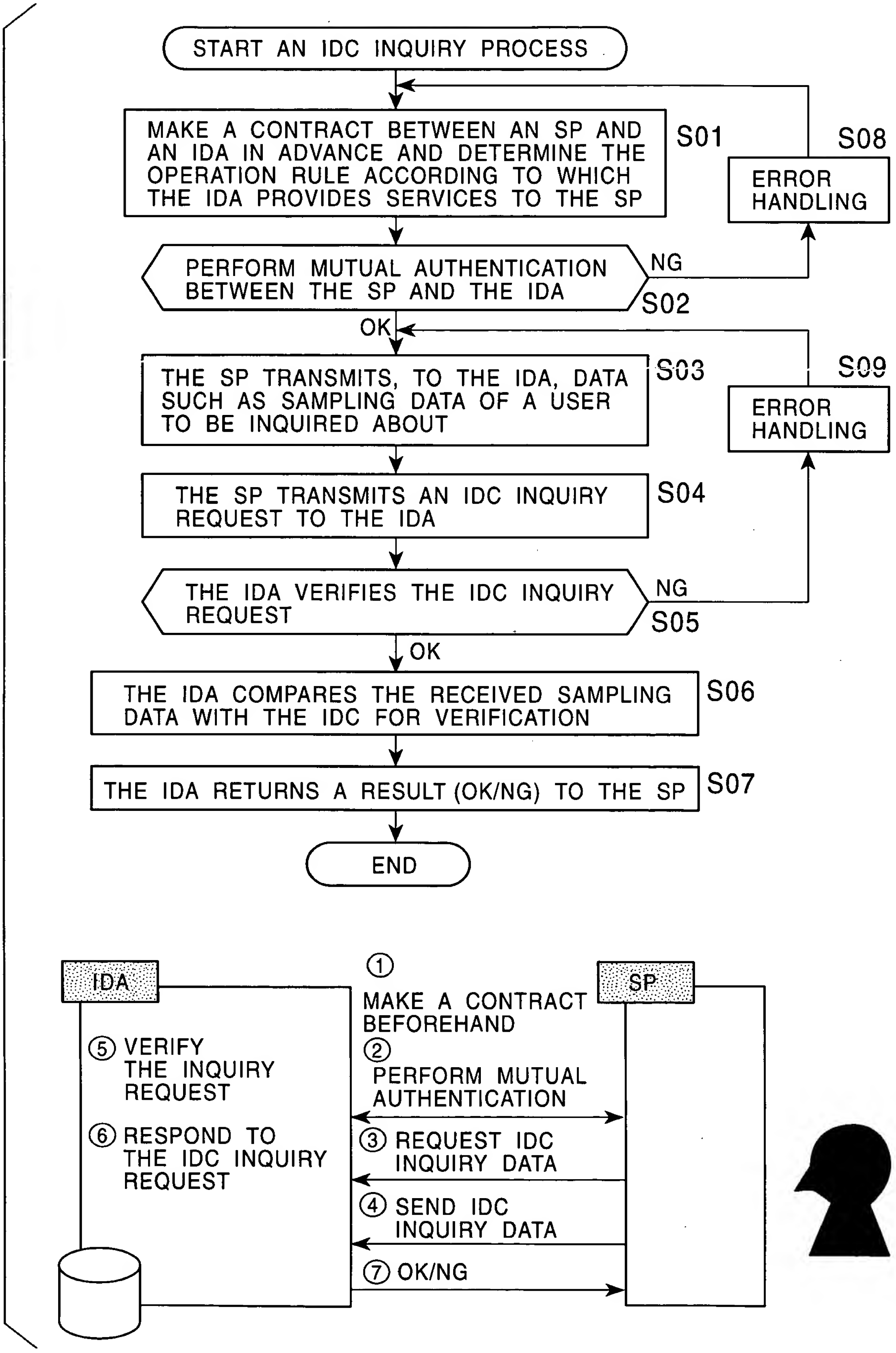

START AN IDC INQUIRY PROCESS
MAKE A CONTRACT BETWEEN AN SP AND AN IDA IN ADVANCE AND DETERMINE THE OPERATION RULE ACCORDING TO WHICH THE IDA PROVIDES SERVICES TO THE SP
S01
S08
ERROR HANDLING
PERFORM MUTUAL AUTHENTICATION BETWEEN THE SP AND THE IDA
NG
S02
OK
THE SP TRANSMITS, TO THE IDA, DATA SUCH AS SAMPLING DATA OF A USER TO BE INQUIRED ABOUT
S03
S09
ERROR HANDLING
THE SP TRANSMITS AN IDC INQUIRY REQUEST TO THE IDA
S04
THE IDA VERIFIES THE IDC INQUIRY REQUEST
NG
S05
OK
THE IDA COMPARES THE RECEIVED SAMPLING DATA WITH THE IDC FOR VERIFICATION
S06
THE IDA RETURNS A RESULT (OK/NG) TO THE SP
S07
END
IDA
SP
① MAKE A CONTRACT BEFOREHAND
② PERFORM MUTUAL AUTHENTICATION
③ REQUEST IDC INQUIRY DATA
④ SEND IDC INQUIRY DATA
⑤ VERIFY THE INQUIRY REQUEST
⑥ RESPOND TO THE IDC INQUIRY REQUEST
⑦ OK/NG

FIG. 19

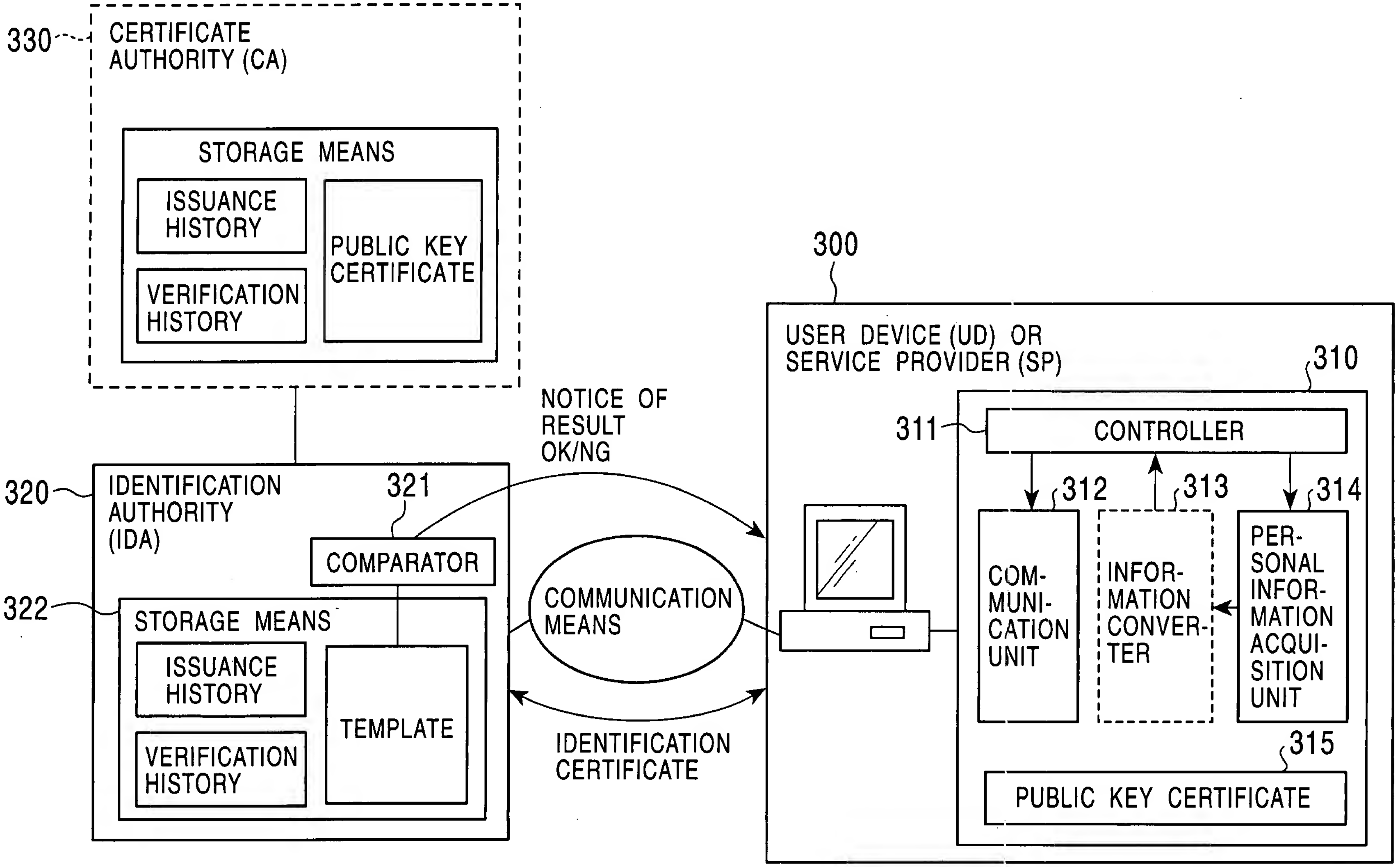

330
CERTIFICATE AUTHORITY (CA)
STORAGE MEANS
ISSUANCE HISTORY
VERIFICATION HISTORY
PUBLIC KEY CERTIFICATE
320
IDENTIFICATION AUTHORITY (IDA)
321
COMPARATOR
322
STORAGE MEANS
ISSUANCE HISTORY
VERIFICATION HISTORY
TEMPLATE
NOTICE OF RESULT OK/NG
COMMUNICATION MEANS
IDENTIFICATION CERTIFICATE
300
USER DEVICE (UD) OR SERVICE PROVIDER (SP)
310
311
CONTROLLER
312
313
314
COM-MUNI-CATION UNIT
INFOR-MATION CONVER-TER
PER-SONAL INFOR-MATION ACQUI-SITION UNIT
315
PUBLIC KEY CERTIFICATE

FIG. 20

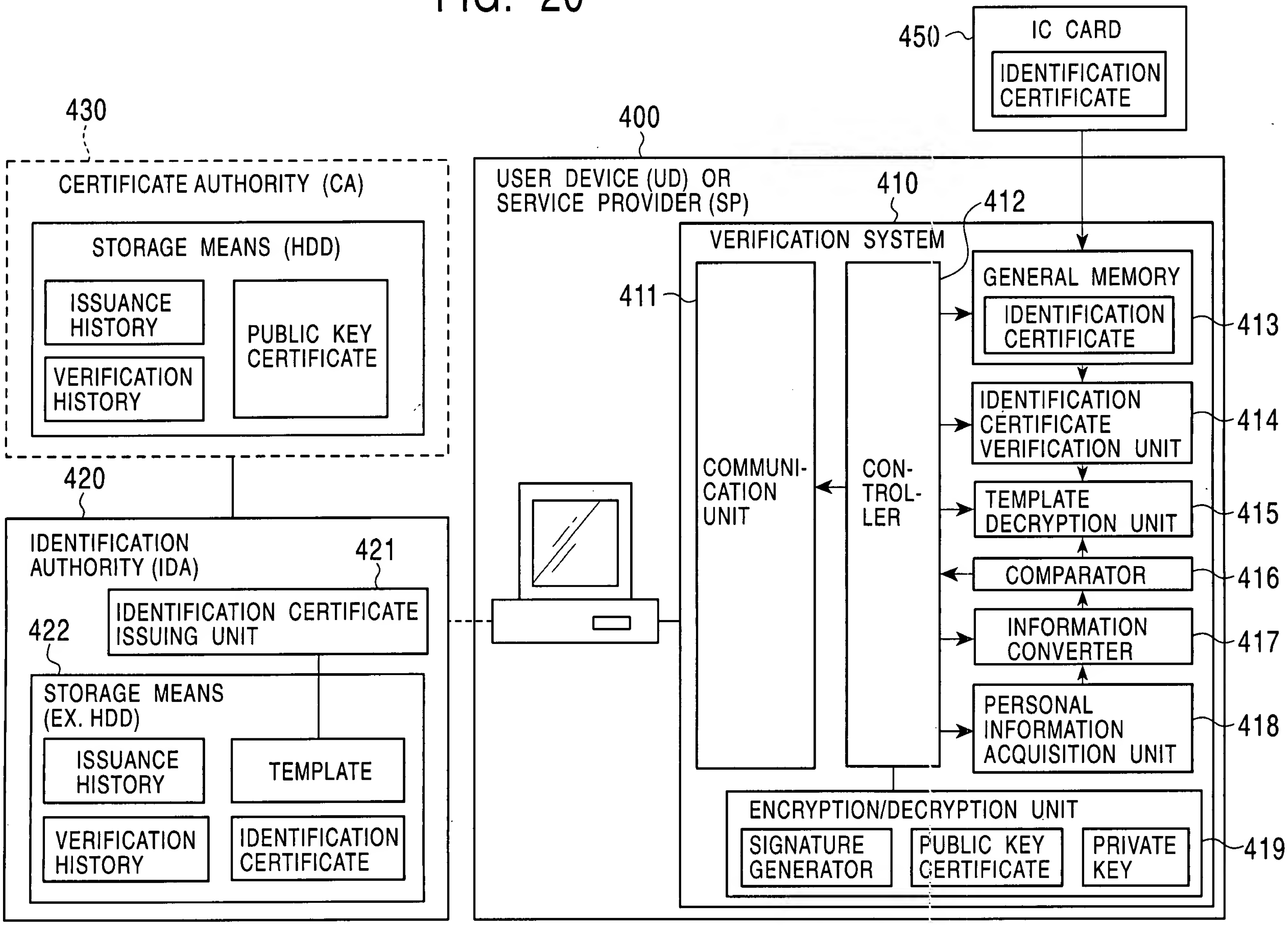

450
IC CARD
IDENTIFICATION CERTIFICATE
430
CERTIFICATE AUTHORITY (CA)
STORAGE MEANS (HDD)
ISSUANCE HISTORY
VERIFICATION HISTORY
PUBLIC KEY CERTIFICATE
400
USER DEVICE (UD) OR SERVICE PROVIDER (SP)
410
VERIFICATION SYSTEM
412
411
COMMUNI-CATION UNIT
CON-TROL-LER
GENERAL MEMORY
IDENTIFICATION CERTIFICATE
413
IDENTIFICATION CERTIFICATE VERIFICATION UNIT
414
TEMPLATE DECRYPTION UNIT
415
COMPARATOR
416
INFORMATION CONVERTER
417
PERSONAL INFORMATION ACQUISITION UNIT
418
ENCRYPTION/DECRYPTION UNIT
SIGNATURE GENERATOR
PUBLIC KEY CERTIFICATE
PRIVATE KEY
419
420
IDENTIFICATION AUTHORITY (IDA)
421
IDENTIFICATION CERTIFICATE ISSUING UNIT
422
STORAGE MEANS (EX. HDD)
ISSUANCE HISTORY
TEMPLATE
VERIFICATION HISTORY
IDENTIFICATION CERTIFICATE

FIG. 21A

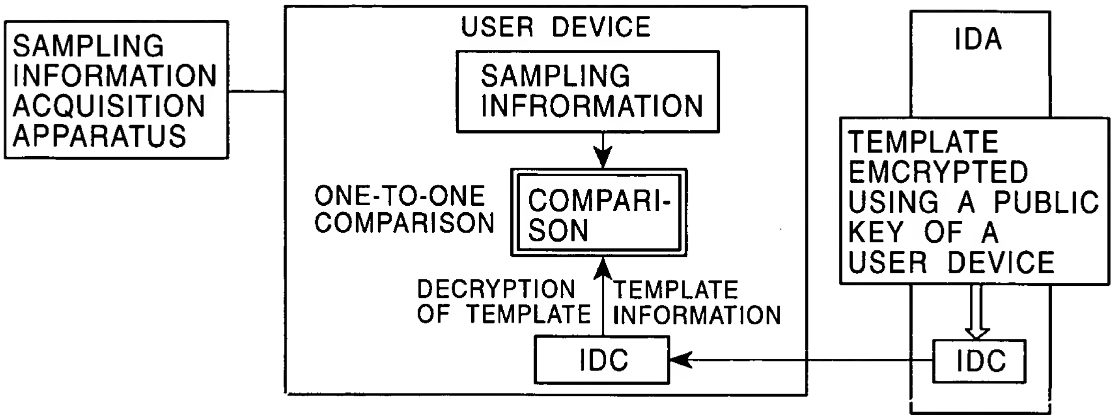


FIG. 21B

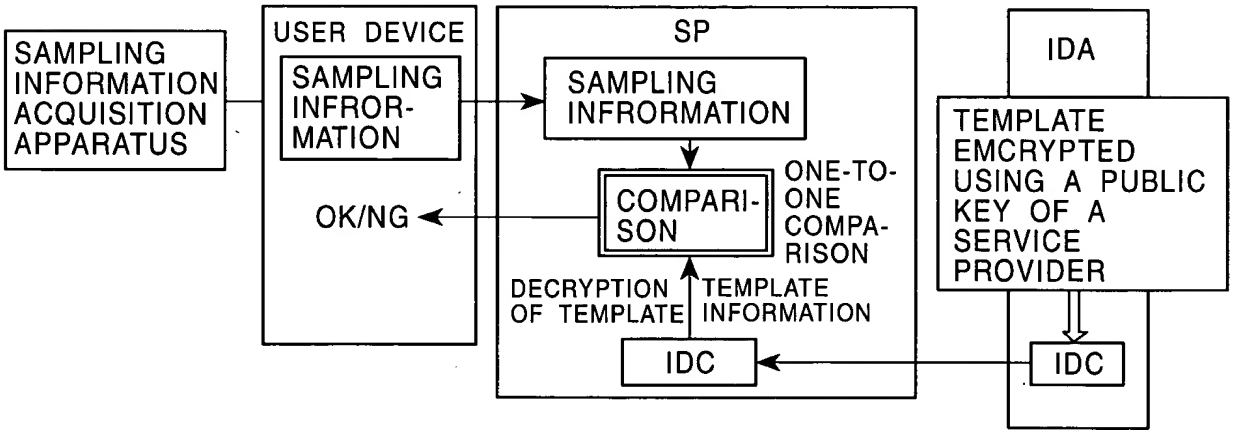


FIG. 21C

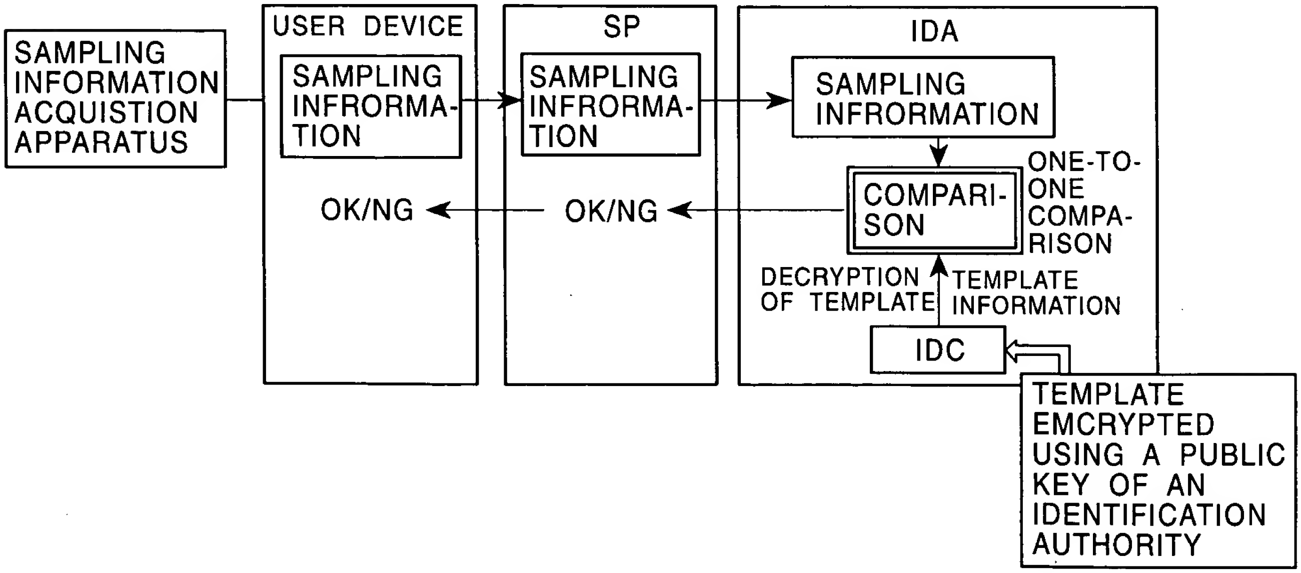


FIG. 22

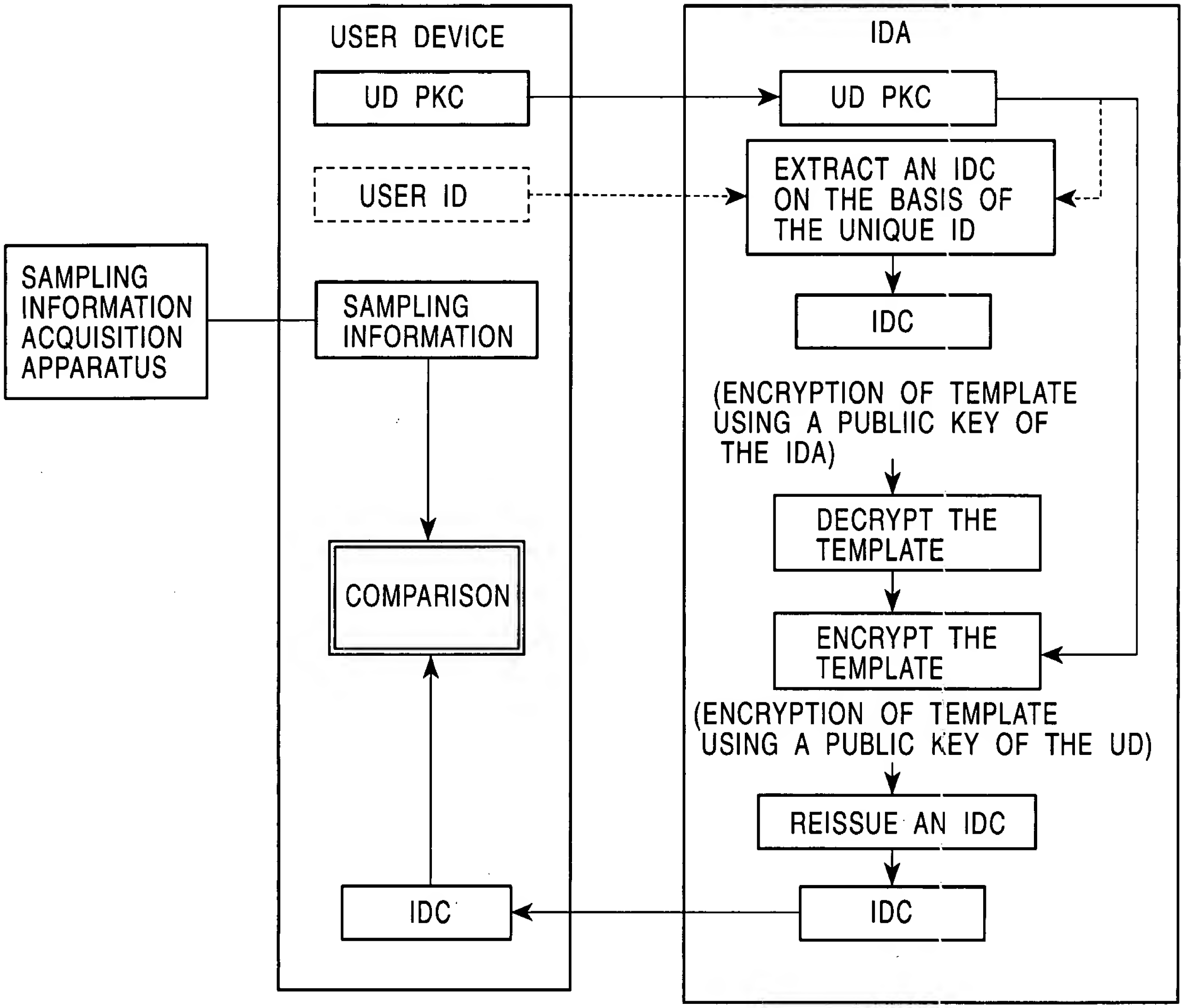

USER DEVICE
UD PKC
USER ID
SAMPLING INFORMATION
SAMPLING INFORMATION ACQUISITION APPARATUS
COMPARISON
IDC
IDA
UD PKC
EXTRACT AN IDC ON THE BASIS OF THE UNIQUE ID
IDC
(ENCRYPTION OF TEMPLATE USING A PUBLIIC KEY OF THE IDA)
DECRYPT THE TEMPLATE
ENCRYPT THE TEMPLATE
(ENCRYPTION OF TEMPLATE USING A PUBLIC KEY OF THE UD)
REISSUE AN IDC
IDC

FIG. 23

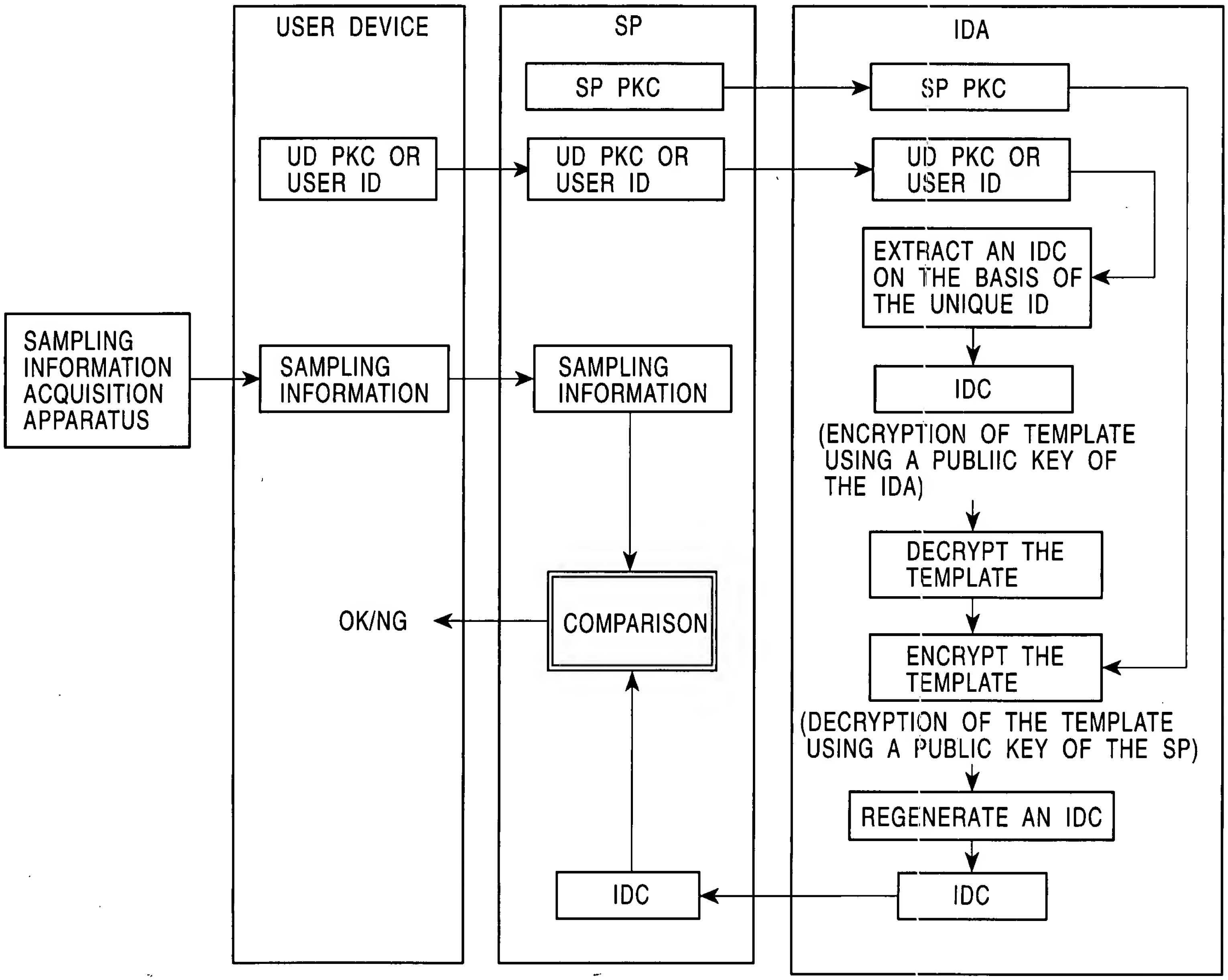

USER DEVICE
SP
IDA
SP PKC
SP PKC
UD PKC OR USER ID
UD PKC OR USER ID
UD PKC OR USER ID
EXTRACT AN IDC ON THE BASIS OF THE UNIQUE ID
SAMPLING INFORMATION ACQUISITION APPARATUS
SAMPLING INFORMATION
SAMPLING INFORMATION
IDC
(ENCRYPTION OF TEMPLATE USING A PUBLIIC KEY OF THE IDA)
DECRYPT THE TEMPLATE
OK/NG
COMPARISON
ENCRYPT THE TEMPLATE
(DECRYPTION OF THE TEMPLATE USING A PUBLIC KEY OF THE SP)
REGENERATE AN IDC
IDC
IDC

FIG. 24

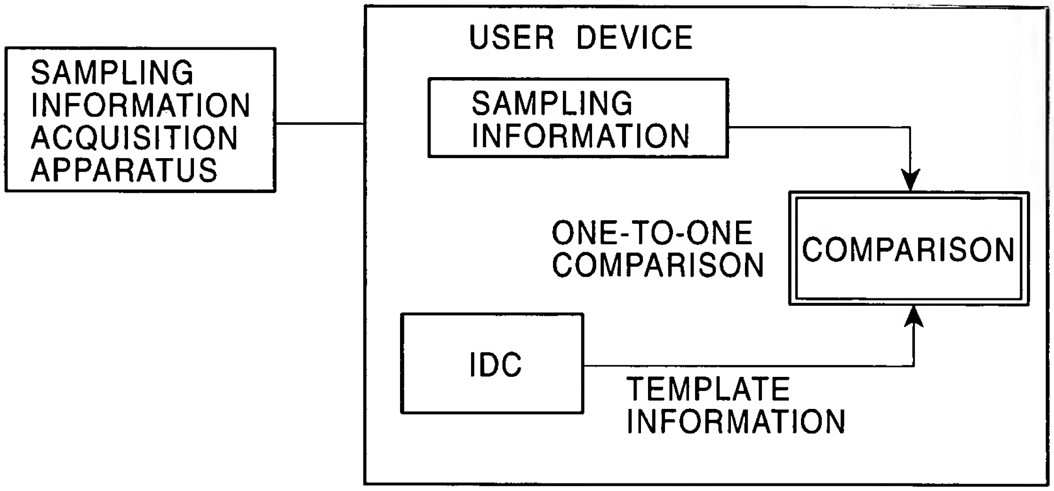

SAMPLING INFORMATION ACQUISITION APPARATUS
USER DEVICE
SAMPLING INFORMATION
ONE-TO-ONE COMPARISON
COMPARISON
IDC
TEMPLATE INFORMATION

FIG. 25

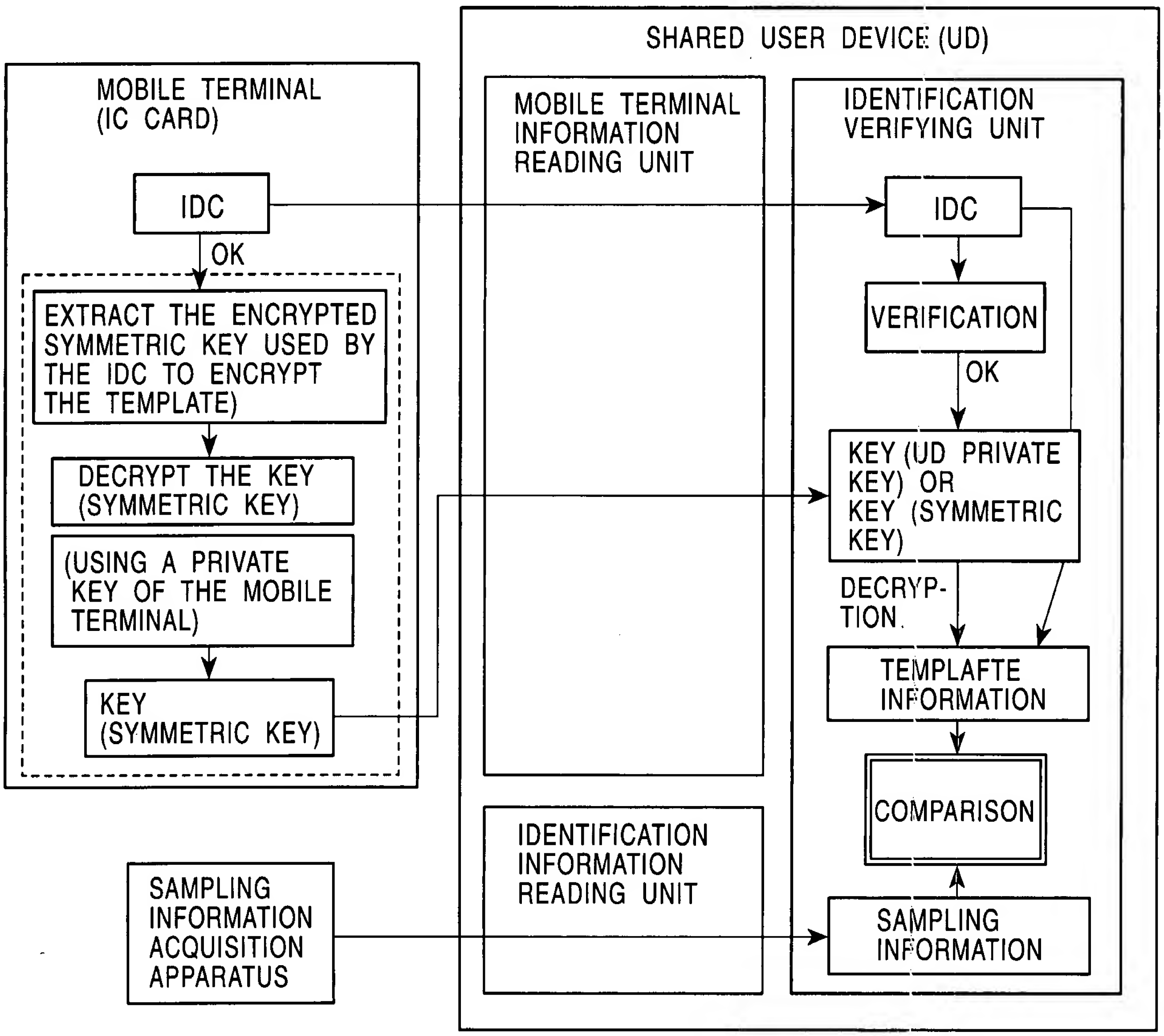

MOBILE TERMINAL (IC CARD)
IDC
OK
EXTRACT THE ENCRYPTED SYMMETRIC KEY USED BY THE IDC TO ENCRYPT THE TEMPLATE)
DECRYPT THE KEY (SYMMETRIC KEY)
(USING A PRIVATE KEY OF THE MOBILE TERMINAL)
KEY (SYMMETRIC KEY)
SAMPLING INFORMATION ACQUISITION APPARATUS
SHARED USER DEVICE (UD)
MOBILE TERMINAL INFORMATION READING UNIT
IDENTIFICATION INFORMATION READING UNIT
IDENTIFICATION VERIFYING UNIT
IDC
VERIFICATION
OK
KEY (UD PRIVATE KEY) OR KEY (SYMMETRIC KEY)
DECRYP-TION.
TEMPLAFTE INFORMATION
COMPARISON
SAMPLING INFORMATION

FIG. 26

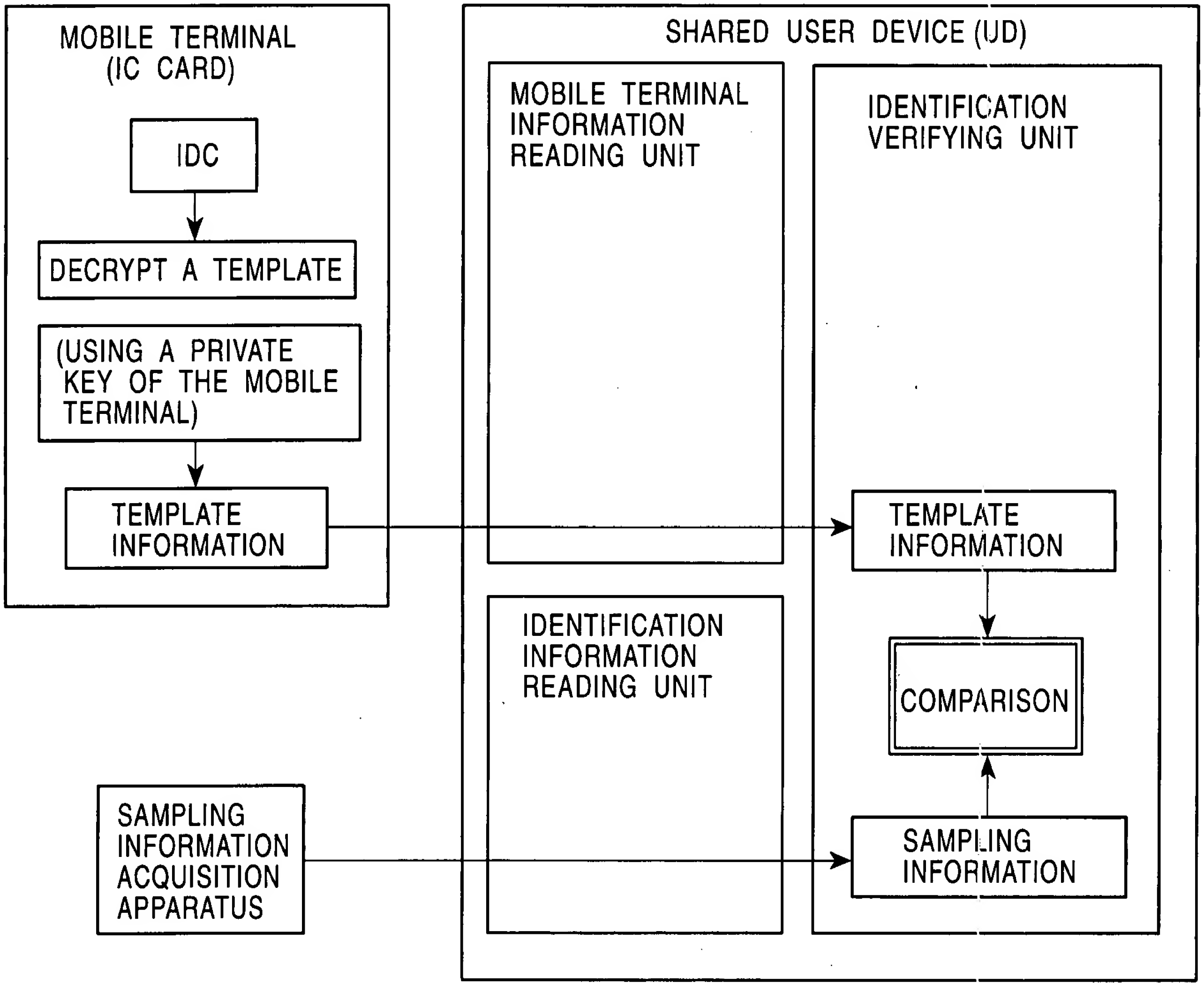

MOBILE TERMINAL (IC CARD)
IDC
DECRYPT A TEMPLATE
(USING A PRIVATE KEY OF THE MOBILE TERMINAL)
TEMPLATE INFORMATION
SAMPLING INFORMATION ACQUISITION APPARATUS
SHARED USER DEVICE (UD)
MOBILE TERMINAL INFORMATION READING UNIT
IDENTIFICATION INFORMATION READING UNIT
IDENTIFICATION VERIFYING UNIT
TEMPLATE INFORMATION
COMPARISON
SAMPLING INFORMATION

FIG. 27

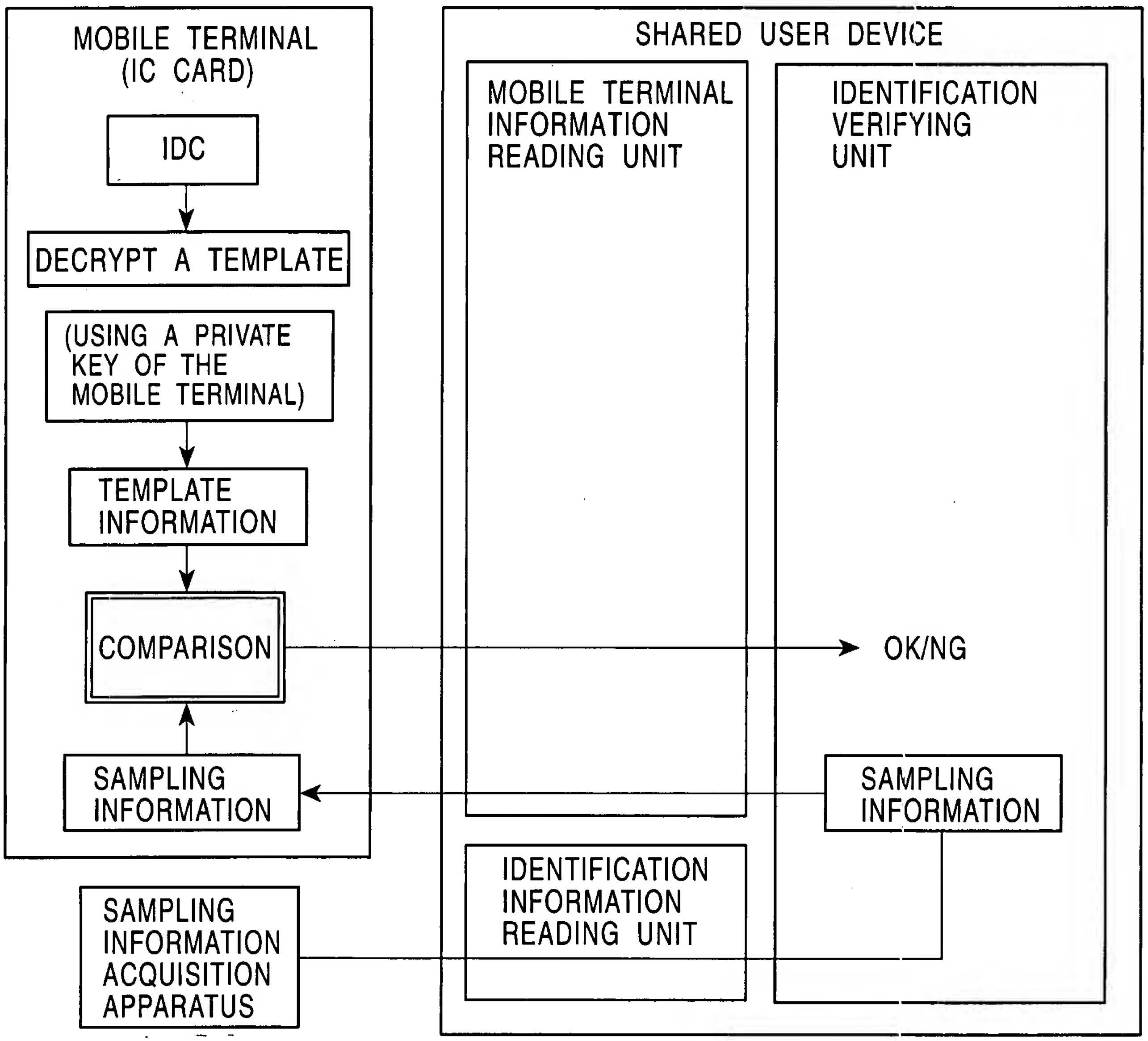

MOBILE TERMINAL
(IC CARD)
IDC
DECRYPT A TEMPLATE
(USING A PRIVATE KEY OF THE MOBILE TERMINAL)
TEMPLATE INFORMATION
COMPARISON
SAMPLING INFORMATION
SAMPLING INFORMATION ACQUISITION APPARATUS
SHARED USER DEVICE
MOBILE TERMINAL INFORMATION READING UNIT
IDENTIFICATION VERIFYING UNIT
OK/NG
SAMPLING INFORMATION
IDENTIFICATION INFORMATION READING UNIT

FIG. 28

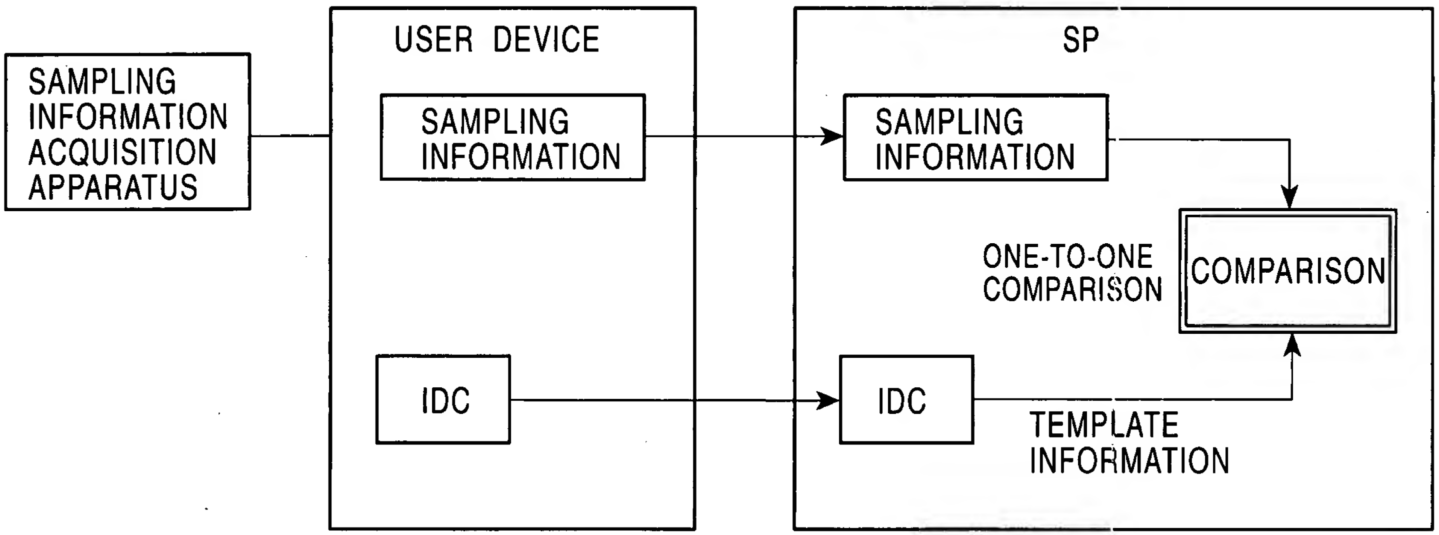

SAMPLING INFORMATION ACQUISITION APPARATUS
USER DEVICE
SAMPLING INFORMATION
IDC
SP
SAMPLING INFORMATION
ONE-TO-ONE COMPARISON
COMPARISON
IDC
TEMPLATE INFORMATION

FIG. 29

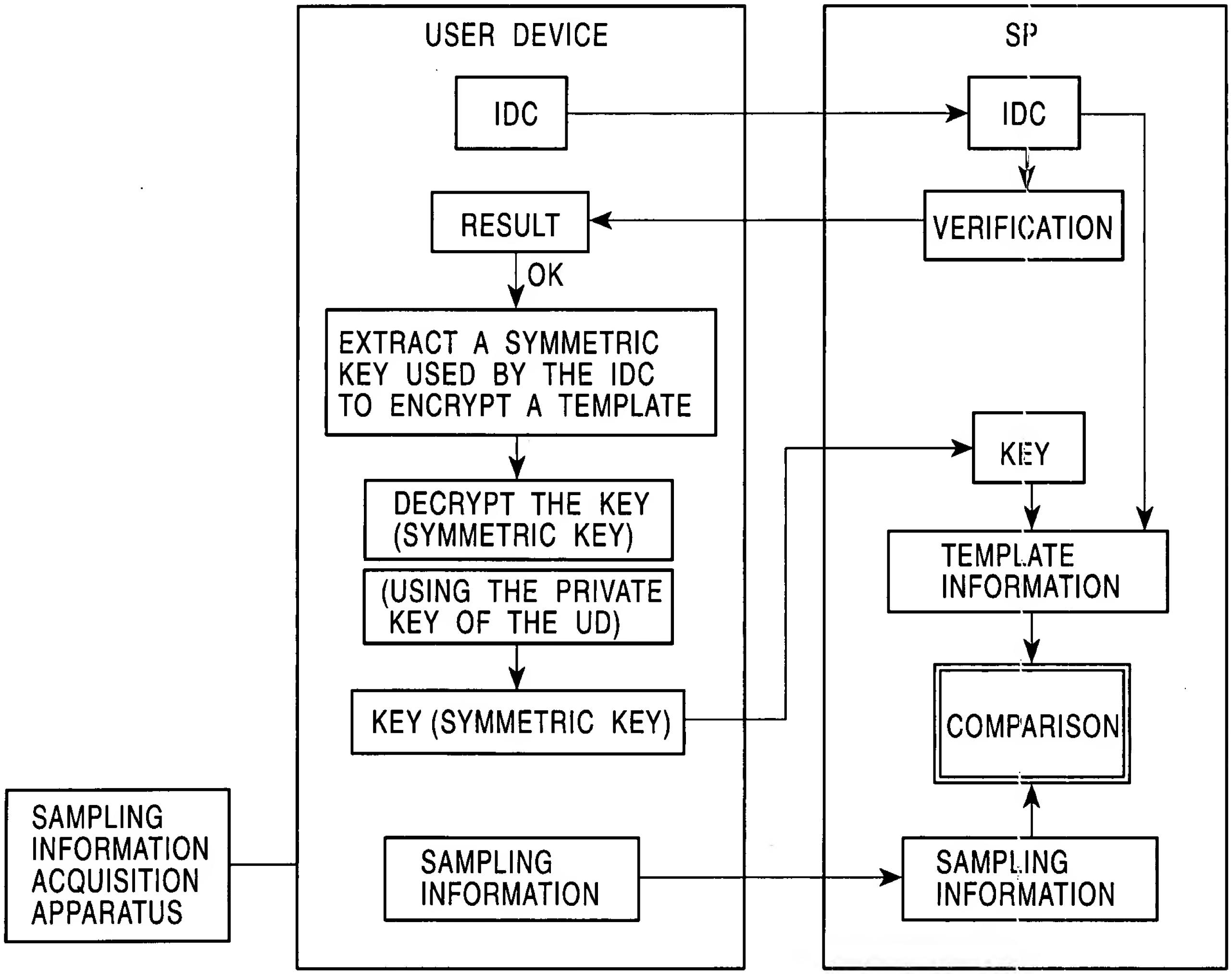

USER DEVICE
IDC
RESULT
OK
EXTRACT A SYMMETRIC KEY USED BY THE IDC TO ENCRYPT A TEMPLATE
DECRYPT THE KEY (SYMMETRIC KEY)
(USING THE PRIVATE KEY OF THE UD)
KEY (SYMMETRIC KEY)
SAMPLING INFORMATION
SAMPLING INFORMATION ACQUISITION APPARATUS
SP
IDC
VERIFICATION
KEY
TEMPLATE INFORMATION
COMPARISON
SAMPLING INFORMATION

FIG. 30

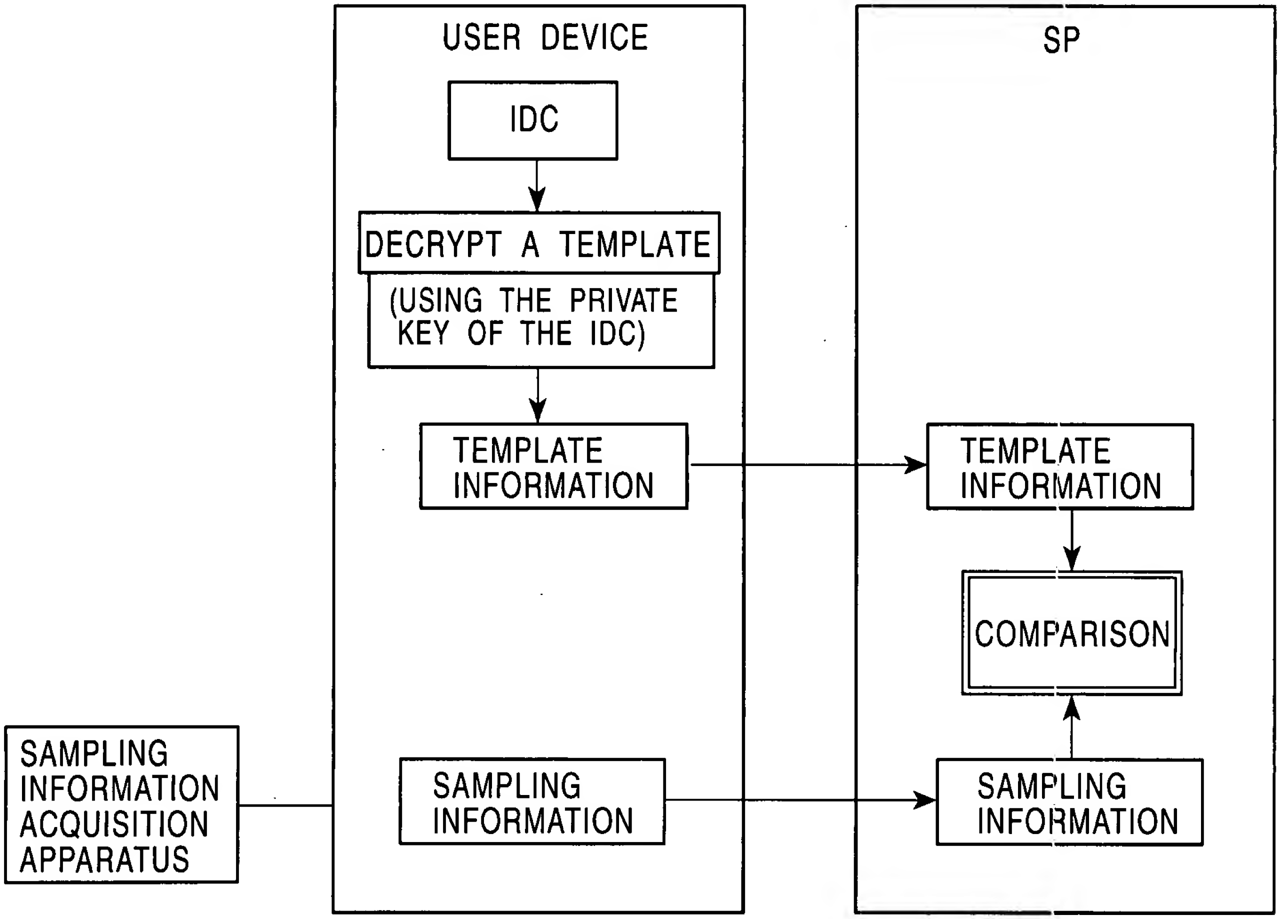

USER DEVICE
IDC
DECRYPT A TEMPLATE
(USING THE PRIVATE KEY OF THE IDC)
TEMPLATE INFORMATION
SAMPLING INFORMATION
SAMPLING INFORMATION ACQUISITION APPARATUS
SP
TEMPLATE INFORMATION
COMPARISON
SAMPLING INFORMATION

FIG. 31

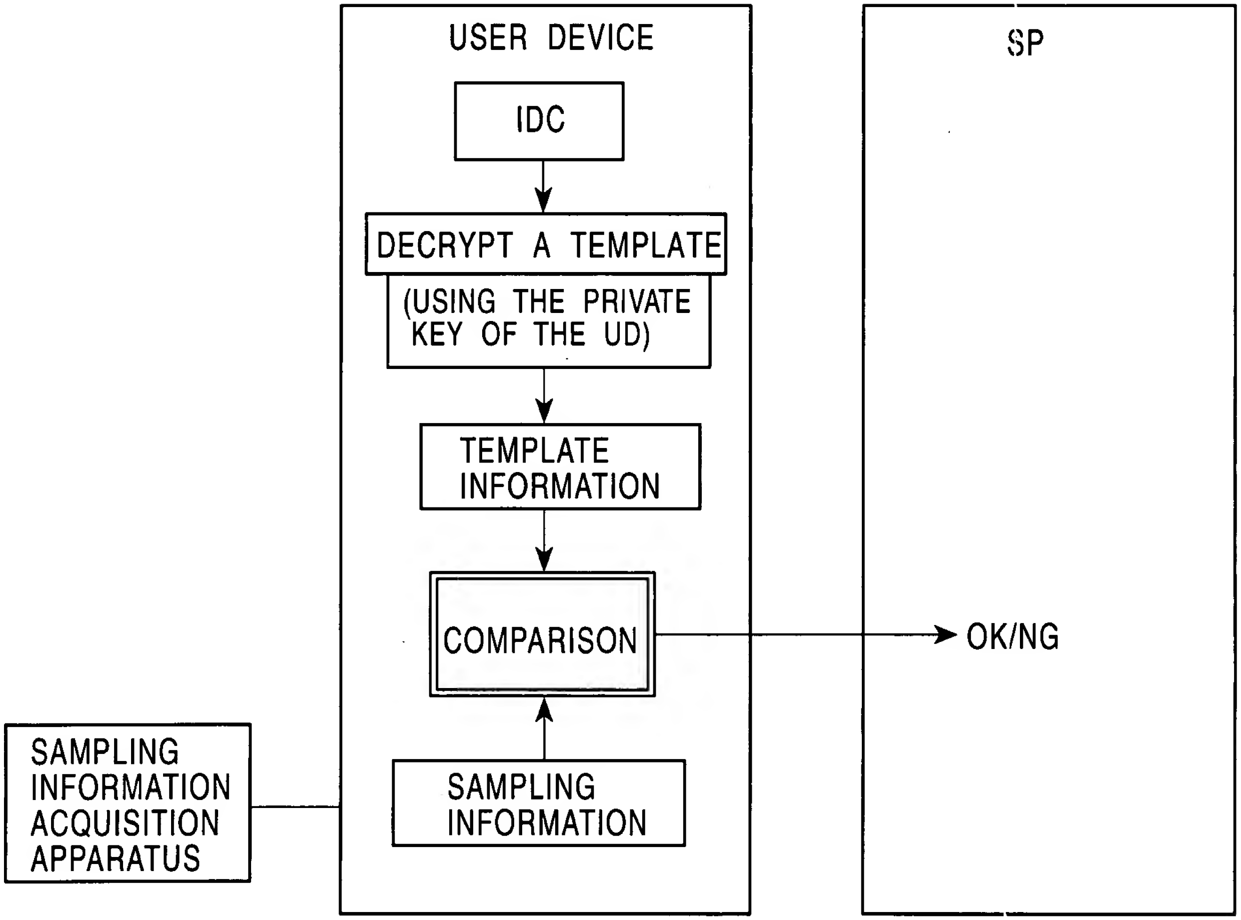

USER DEVICE
IDC
DECRYPT A TEMPLATE
(USING THE PRIVATE KEY OF THE UD)
TEMPLATE INFORMATION
COMPARISON
SAMPLING INFORMATION
SAMPLING INFORMATION ACQUISITION APPARATUS
SP
OK/NG

FIG. 32

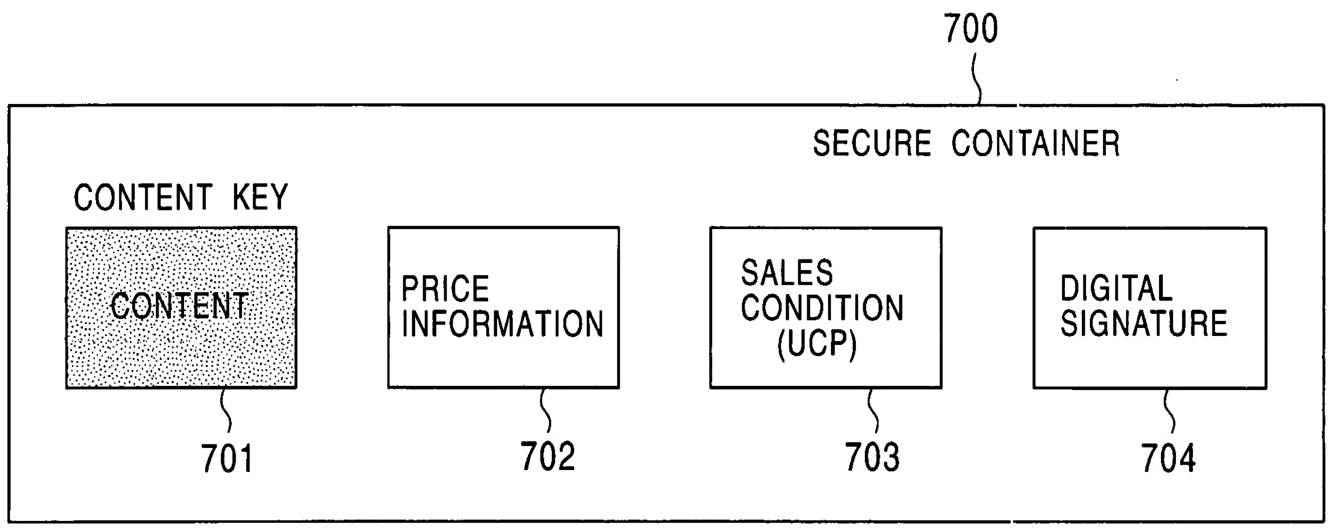

700
SECURE CONTAINER
CONTENT KEY
CONTENT
701
PRICE INFORMATION
702
SALES CONDITION (UCP)
703
DIGITAL SIGNATURE
704

FIG. 33

USER ID	IDENTIFICATION CERTIFICATE (IDC) IDENTIFIER
ABC0001	CDE00021
ABC0002	CDE00027
ABC0003	CDE03211
⋮	⋮
BBC0231	EED02333

FIG. 34

DATA TYPE		
TYPE OF DEALING POLICY		
PERIOD DURING WHICH DEALING POLICY IS VALID		
CONTENT ID		
CONTENT PROVIDER ID		
DEALING POLICY ID		
VERSION OF THE DEALING POLICY		
AREA CODE		
USABLE DEVICE CONDITIONS		
USERS PERMITTED TO USE THE CONTENT		
IDC IDENTIFIER LIST		711
SERVICE PROVIDER ID		
UCP GENERATION MANAGEMENT INFORMATION		712
MAXIMUM ALLOWABLE NUMBER OF SECONDARY DISTRIBUTIONS		713
NUMBER OF RULES		
RULE ADDRESS		
RULE 1	RULE NUMBER	
	TYPE OF PERMITTED USAGE	
	⋮	
⋮	⋮	
RULE N	RULE NUMBER	
	TYPE OF PERMITTED USAGE	
	⋮	
(INDICATION OF WHETHER THE SIGNATURE HAS BEEN VERIFIED)		
PUBLIC KEY CERTIFICATE		
SIGNATURE		

FIG. 35

RULE NUMBER	PERMITTED USAGE	PERIOD	NUMBER OF TIMES CONTENT IS USED	COPY
1	PLAYBACK	NOT LIMITED	NOT LIMITED	—
2		LIMITED	NOT LIMITED	—
3		NOT LIMITED	LIMITED	—
4	COPY	NOT LIMITED	NOT LIMITED	NOT LIMITED
5		LIMITED	NOT LIMITED	NOT LIMITED
6		NOT LIMITED	LIMITED	NOT LIMITED
7		NOT LIMITED	NOT LIMITED	SCMS
8		LIMITED	NOT LIMITED	
9		NOT LIMITED	LIMITED	
10		NOT LIMITED	NOT LIMITED	OTHERS
11		LIMITED	NOT LIMITED	
12		NOT LIMITED	LIMITED	
13	CHANGING OF PERMITTED USAGE			
14	REDISTRIBUTION			
15	UPGRADE TO AN ALBUM			
16	PERMISSION OF TRANSFERRING MANAGEMENT			

FIG. 36

DATA TYPE		
TYPE OF PRICE INFORMATION		
PERIOD DURING WHICH THE PRICE INFORMATION IS VALID		
CONTENT ID		
SERVICE PROVIDER ID		
PRICE INFORMATION ID		
VERSION OF THE PRICE INFORMATION		
AREA CODE		
USABLE DEVICE CONDITIONS		
USERS PERMITTED TO USE THE CONTENT		
IDC IDENTIFIER LIST		721
CONTENT PROVIDER ID		
DEALING POLICY ID		
NUMBER OF RULES		
RULE ADDRESS		
RULE 1	RULE NUMBER	
	⋮	
	⋮	
⋮	⋮	
RULE N	RULE NUMBER	
	⋮	
	⋮	
(INDICATION OF WHETHER THE SIGNATURE HAS BEEN VERIFIED)		
PUBLIC KEY CERTIFICATE		
SIGNATURE		

FIG. 37

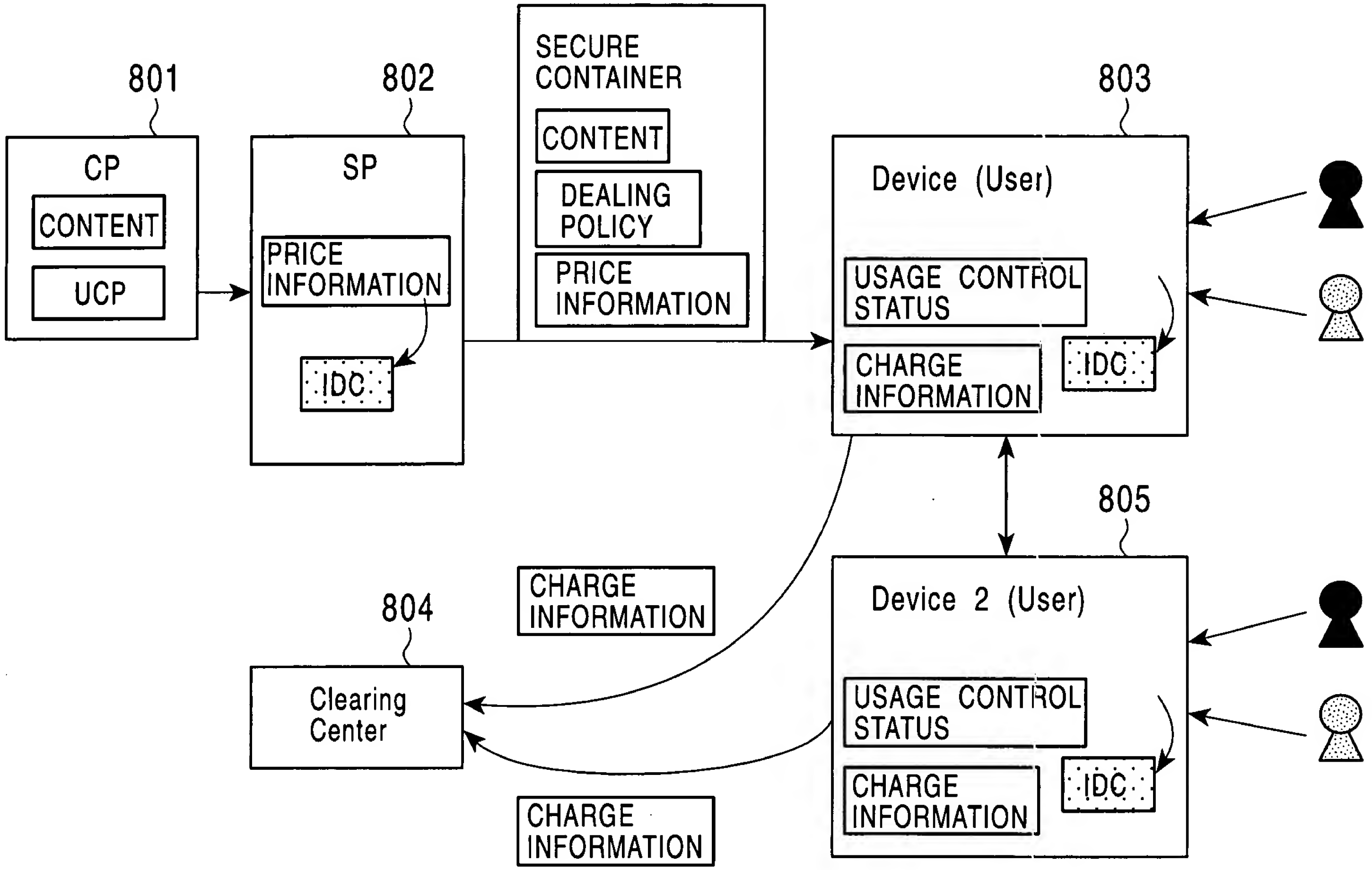

801
CP
CONTENT
UCP
802
SP
PRICE INFORMATION
IDC
SECURE CONTAINER
CONTENT
DEALING POLICY
PRICE INFORMATION
803
Device (User)
USAGE CONTROL STATUS
CHARGE INFORMATION
IDC
805
Device 2 (User)
USAGE CONTROL STATUS
CHARGE INFORMATION
IDC
804
Clearing Center
CHARGE INFORMATION
CHARGE INFORMATION

FIG. 38

DATA TYPE	
TYPE OF USAGE PERMISSION CONDITION INFORMATION	
PERIOD DURING WHICH THE USAGE PERMISSION CONDITION INFORMATION IS VALID	
CONTENT ID	
ALBUM ID	
ENCRYPTION PROCESSING UNIT ID	
USER ID	
CONTENT PROVIDER ID	
DEALINGF POLICY ID	
VERSION OF DEALING POLICY	
SERVICE PROVIDER ID	
PRICE INFORMATION ID	
VERSION OF PRICE INFORMATION	
ID OF USAGE PERMISSION CONDITION INFORMATION	
RULE NUMBER OF PERMISSION FOR PLAYBACK (USAGE)	
PERMITTED USAGE NUMBER	
NUMBER OF TIMES THE CONTENT IS ALLOWED TO BE FURTHER PLAYED BACK	
PERIOD DURING WICH THE PLAYBACK PERMISSION IS VALID	
RULE NUMBER OF PERMISSION FOR COPYING (USE)	
USAGE PERMISSION NUMBER	
NUMBER OF TIMES THE CONTENT IS ALLOWED TO BE FURTHER COPIED	
UCS GENERATION MANAGEMENT INFORMATION	732
NUMBER OF TIMES UCS IS ALLOWED TO BE SECONDARILY DISTRIBUTED	733
IDC IDENTIFIER LIST	731
ID OF THE ENCRYPTION PROCESSING UNIT HAVING PERMISSION IN TERMS OF PLAYBACK	

FIG. 39

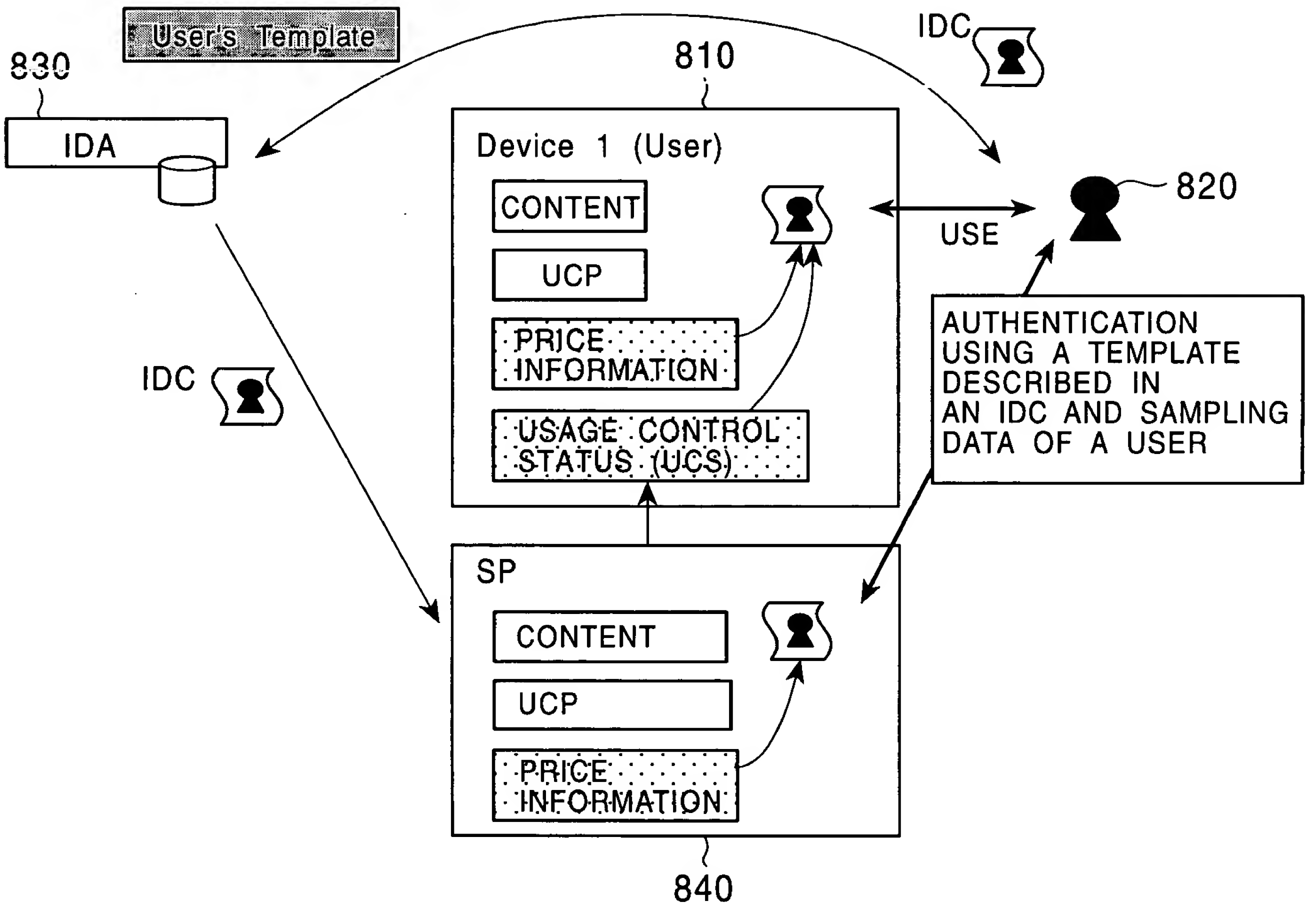

User's Template
830
IDA
IDC
810
Device 1 (User)
CONTENT
UCP
PRICE INFORMATION
USAGE CONTROL STATUS (UCS)
USE
820
AUTHENTICATION USING A TEMPLATE DESCRIBED IN AN IDC AND SAMPLING DATA OF A USER
IDC
SP
CONTENT
UCP
PRICE INFORMATION
840

FIG. 40

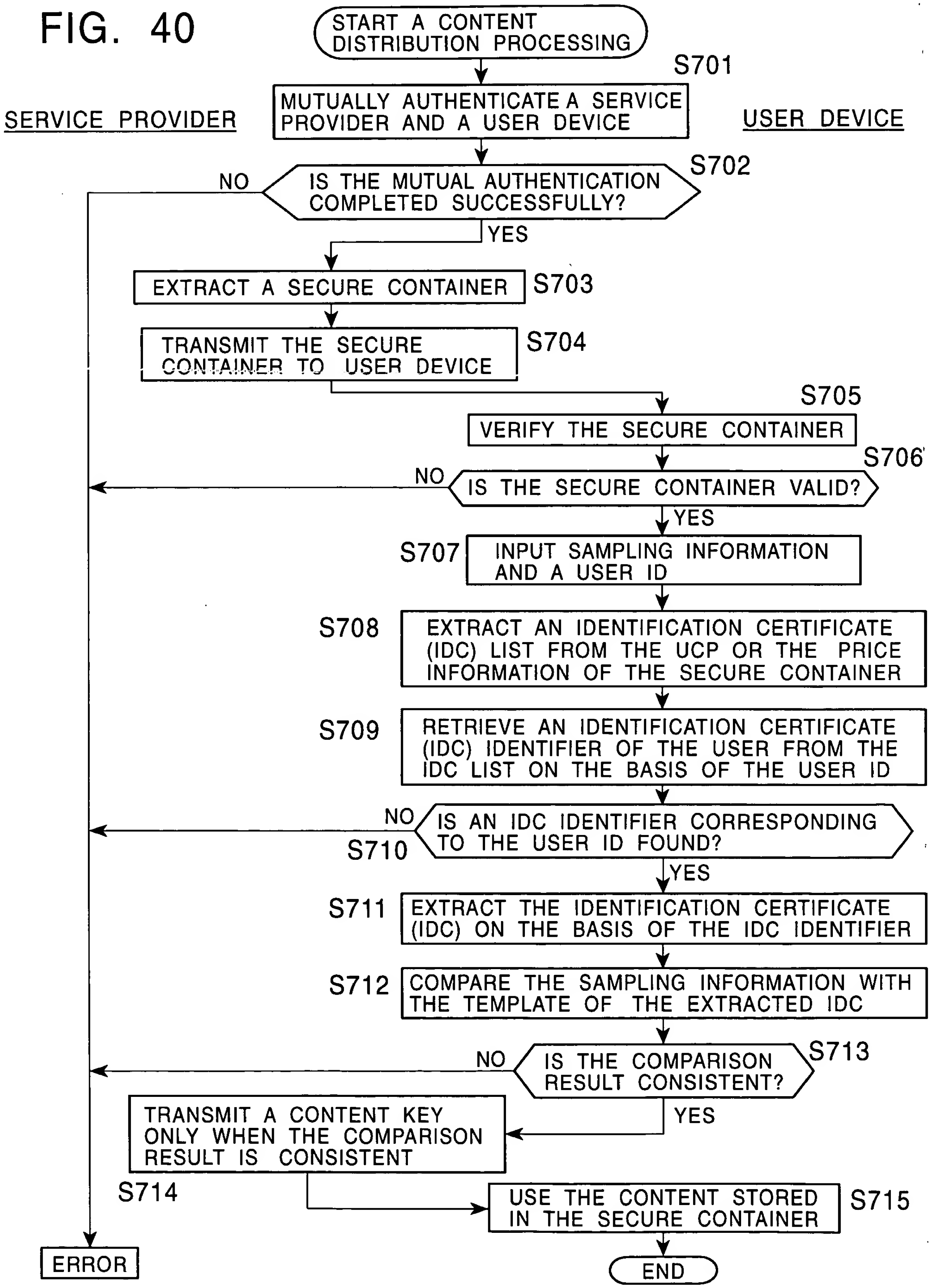

START A CONTENT DISTRIBUTION PROCESSING
SERVICE PROVIDER
USER DEVICE
S701
MUTUALLY AUTHENTICATE A SERVICE PROVIDER AND A USER DEVICE
S702
IS THE MUTUAL AUTHENTICATION COMPLETED SUCCESSFULLY?
NO
YES
S703
EXTRACT A SECURE CONTAINER
S704
TRANSMIT THE SECURE CONTAINER TO USER DEVICE
S705
VERIFY THE SECURE CONTAINER
S706
IS THE SECURE CONTAINER VALID?
NO
YES
S707
INPUT SAMPLING INFORMATION AND A USER ID
S708
EXTRACT AN IDENTIFICATION CERTIFICATE (IDC) LIST FROM THE UCP OR THE PRICE INFORMATION OF THE SECURE CONTAINER
S709
RETRIEVE AN IDENTIFICATION CERTIFICATE (IDC) IDENTIFIER OF THE USER FROM THE IDC LIST ON THE BASIS OF THE USER ID
NO
IS AN IDC IDENTIFIER CORRESPONDING TO THE USER ID FOUND?
S710
YES
S711
EXTRACT THE IDENTIFICATION CERTIFICATE (IDC) ON THE BASIS OF THE IDC IDENTIFIER
S712
COMPARE THE SAMPLING INFORMATION WITH THE TEMPLATE OF THE EXTRACTED IDC
NO
IS THE COMPARISON RESULT CONSISTENT?
S713
YES
TRANSMIT A CONTENT KEY ONLY WHEN THE COMPARISON RESULT IS CONSISTENT
S714
USE THE CONTENT STORED IN THE SECURE CONTAINER
S715
ERROR
END

FIG. 41

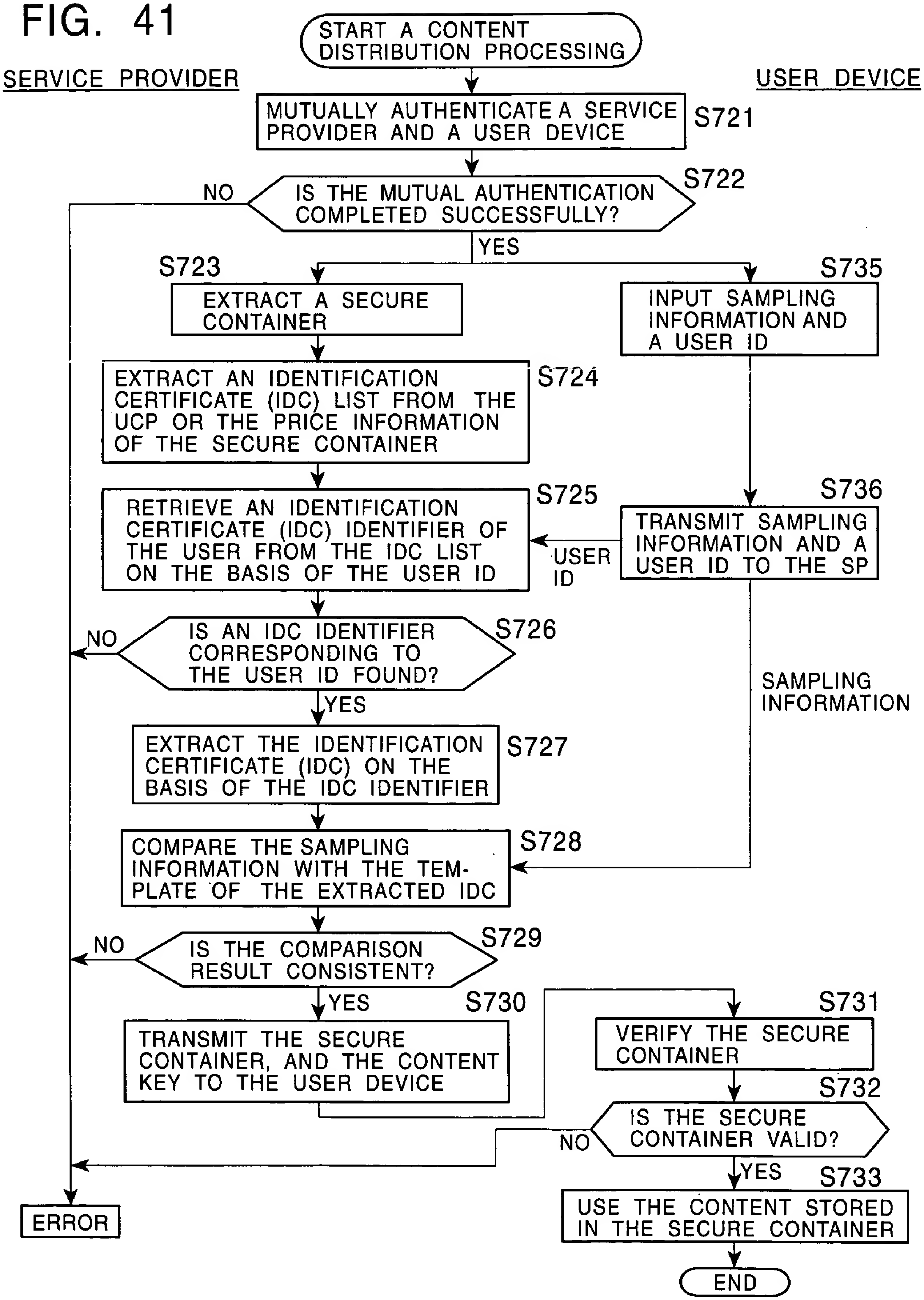
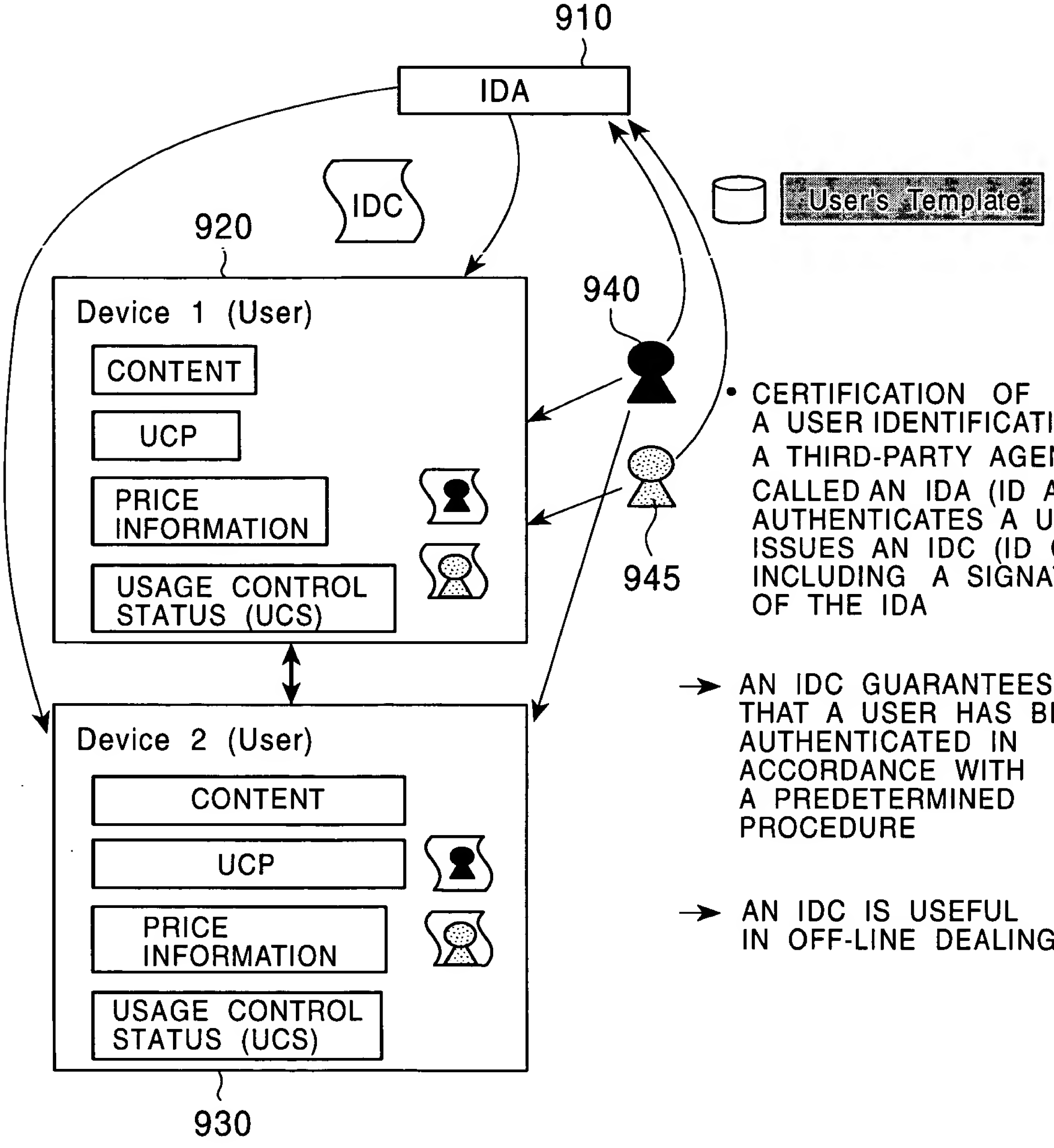

SERVICE PROVIDER
USER DEVICE
START A CONTENT DISTRIBUTION PROCESSING
MUTUALLY AUTHENTICATE A SERVICE PROVIDER AND A USER DEVICE
S721
IS THE MUTUAL AUTHENTICATION COMPLETED SUCCESSFULLY?
S722
NO
YES
S723
EXTRACT A SECURE CONTAINER
S735
INPUT SAMPLING INFORMATION AND A USER ID
EXTRACT AN IDENTIFICATION CERTIFICATE (IDC) LIST FROM THE UCP OR THE PRICE INFORMATION OF THE SECURE CONTAINER
S724
RETRIEVE AN IDENTIFICATION CERTIFICATE (IDC) IDENTIFIER OF THE USER FROM THE IDC LIST ON THE BASIS OF THE USER ID
S725
USER ID
S736
TRANSMIT SAMPLING INFORMATION AND A USER ID TO THE SP
IS AN IDC IDENTIFIER CORRESPONDING TO THE USER ID FOUND?
S726
NO
YES
SAMPLING INFORMATION
EXTRACT THE IDENTIFICATION CERTIFICATE (IDC) ON THE BASIS OF THE IDC IDENTIFIER
S727
COMPARE THE SAMPLING INFORMATION WITH THE TEMPLATE OF THE EXTRACTED IDC
S728
IS THE COMPARISON RESULT CONSISTENT?
S729
NO
YES
S730
TRANSMIT THE SECURE CONTAINER, AND THE CONTENT KEY TO THE USER DEVICE
S731
VERIFY THE SECURE CONTAINER
S732
IS THE SECURE CONTAINER VALID?
NO
YES
S733
USE THE CONTENT STORED IN THE SECURE CONTAINER
END
ERROR

FIG. 42



- CERTIFICATION OF A USER IDENTIFICATION: IDC

A THIRD-PARTY AGENCY CALLED AN IDA (ID AUTHORITY) AUTHENTICATES A USER AND ISSUES AN IDC (ID CERTIFICATE) INCLUDING A SIGNATURE OF THE IDA

→ AN IDC GUARANTEES THAT A USER HAS BEEN AUTHENTICATED IN ACCORDANCE WITH A PREDETERMINED PROCEDURE

→ AN IDC IS USEFUL IN OFF-LINE DEALINGS

FIG. 43

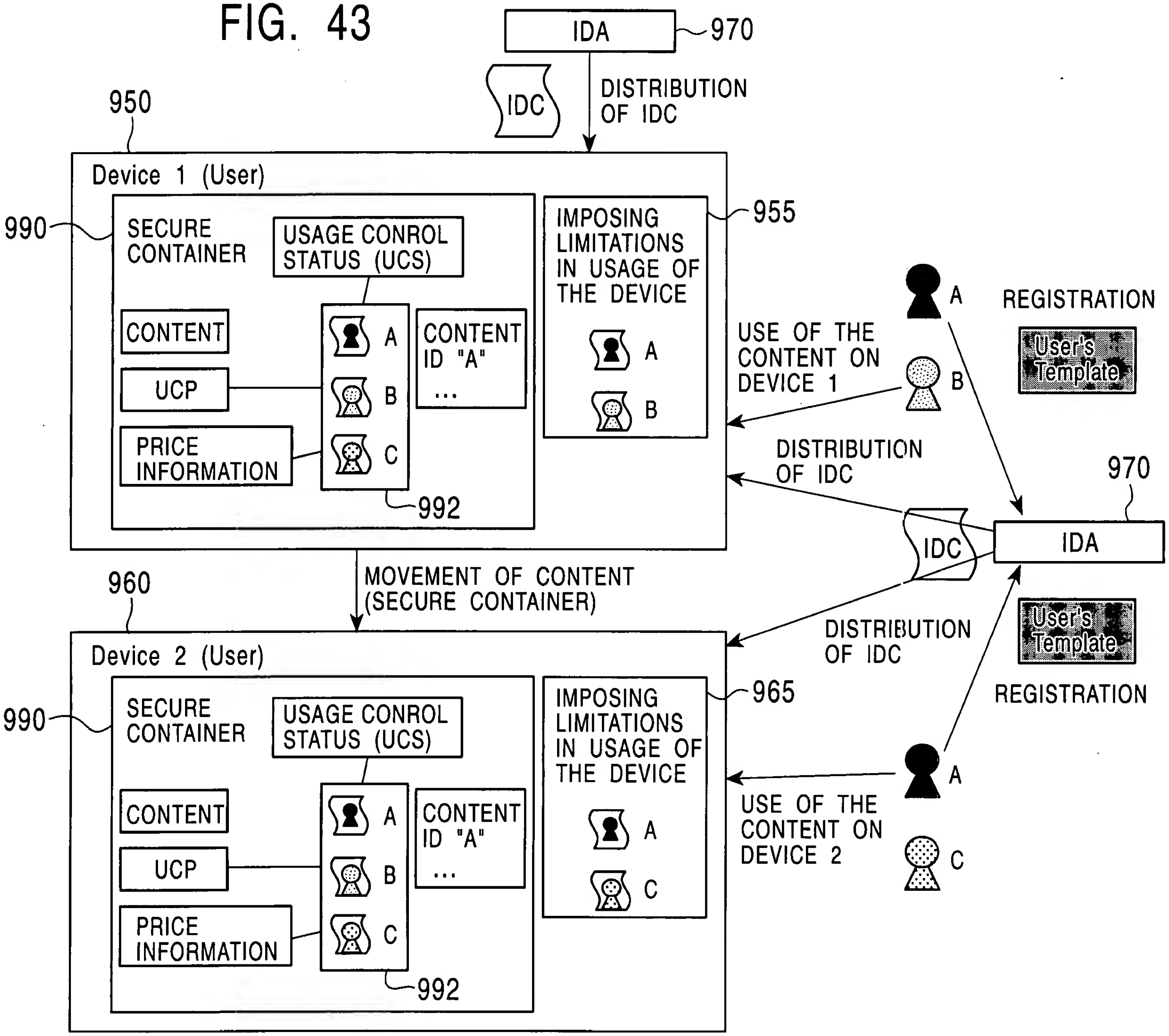

IDA
970
IDC
DISTRIBUTION OF IDC
950
Device 1 (User)
990
SECURE CONTAINER
USAGE CONROL STATUS (UCS)
CONTENT
UCP
PRICE INFORMATION
A
B
C
992
CONTENT ID "A" ...
IMPOSING LIMITATIONS IN USAGE OF THE DEVICE
A
B
955
USE OF THE CONTENT ON DEVICE 1
DISTRIBUTION OF IDC
A
B
REGISTRATION
User's Template
970
IDA
IDC
MOVEMENT OF CONTENT (SECURE CONTAINER)
960
Device 2 (User)
990
SECURE CONTAINER
USAGE CONROL STATUS (UCS)
CONTENT
UCP
PRICE INFORMATION
A
B
C
992
CONTENT ID "A" ...
IMPOSING LIMITATIONS IN USAGE OF THE DEVICE
A
C
965
DISTRIBUTION OF IDC
User's Template
REGISTRATION
USE OF THE CONTENT ON DEVICE 2
A
C

FIG. 44

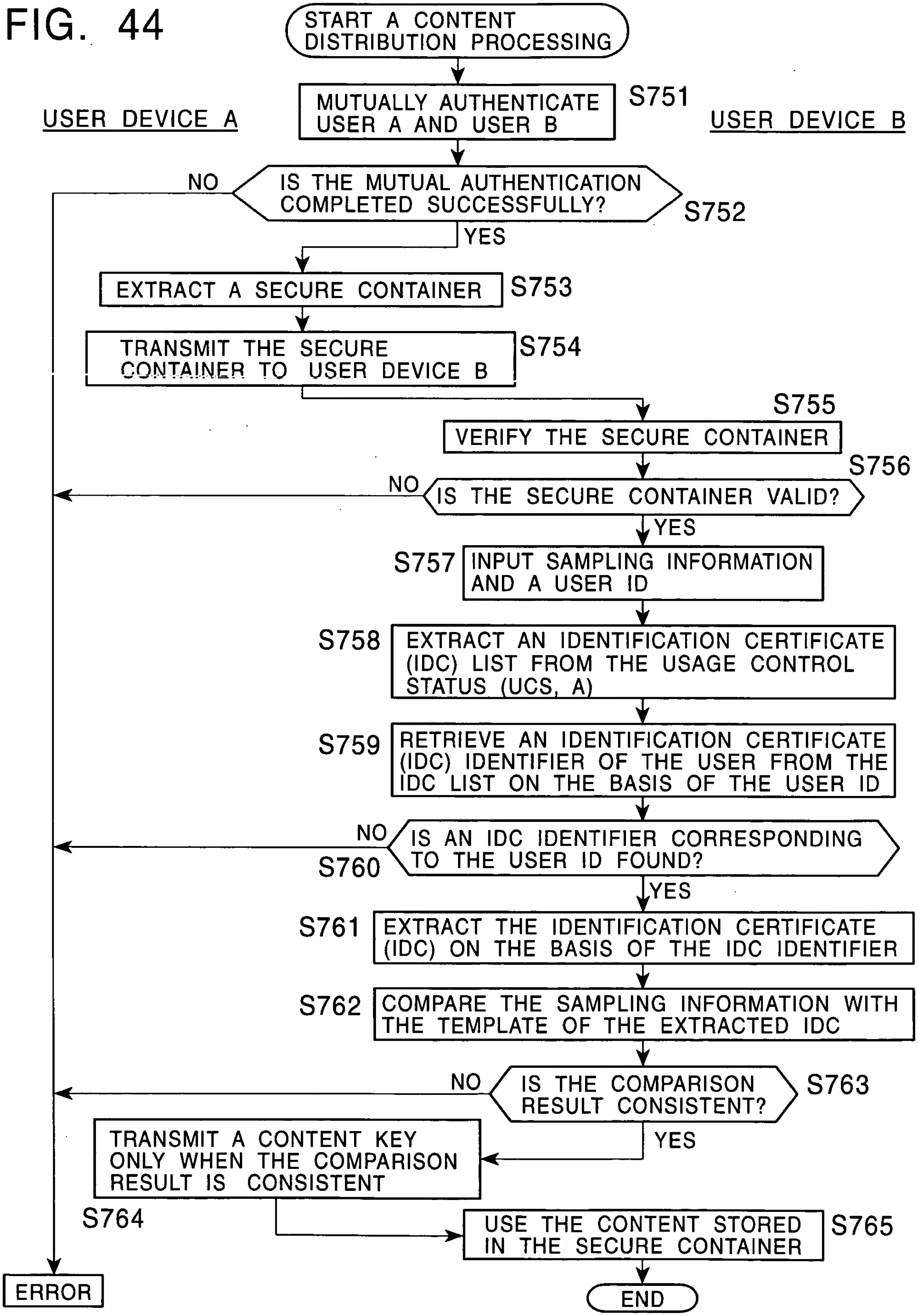

START A CONTENT DISTRIBUTION PROCESSING
USER DEVICE A
USER DEVICE B
MUTUALLY AUTHENTICATE USER A AND USER B
S751
IS THE MUTUAL AUTHENTICATION COMPLETED SUCCESSFULLY?
S752
NO
YES
EXTRACT A SECURE CONTAINER
S753
TRANSMIT THE SECURE CONTAINER TO USER DEVICE B
S754
S755
VERIFY THE SECURE CONTAINER
S756
IS THE SECURE CONTAINER VALID?
NO
YES
S757
INPUT SAMPLING INFORMATION AND A USER ID
S758
EXTRACT AN IDENTIFICATION CERTIFICATE (IDC) LIST FROM THE USAGE CONTROL STATUS (UCS, A)
S759
RETRIEVE AN IDENTIFICATION CERTIFICATE (IDC) IDENTIFIER OF THE USER FROM THE IDC LIST ON THE BASIS OF THE USER ID
NO
IS AN IDC IDENTIFIER CORRESPONDING TO THE USER ID FOUND?
S760
YES
S761
EXTRACT THE IDENTIFICATION CERTIFICATE (IDC) ON THE BASIS OF THE IDC IDENTIFIER
S762
COMPARE THE SAMPLING INFORMATION WITH THE TEMPLATE OF THE EXTRACTED IDC
NO
IS THE COMPARISON RESULT CONSISTENT?
S763
YES
TRANSMIT A CONTENT KEY ONLY WHEN THE COMPARISON RESULT IS CONSISTENT
S764
USE THE CONTENT STORED IN THE SECURE CONTAINER
S765
ERROR
END

FIG. 45

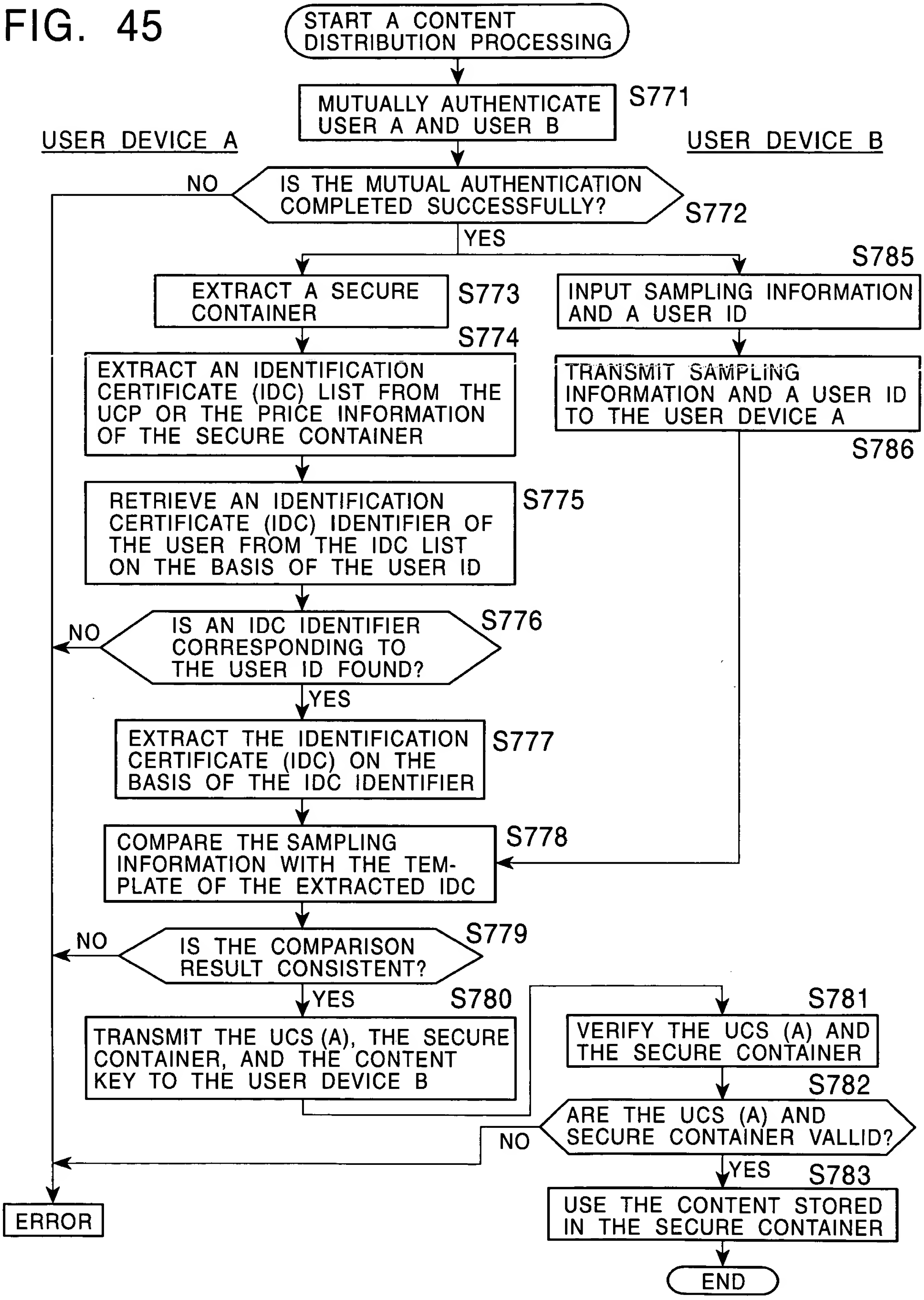

START A CONTENT DISTRIBUTION PROCESSING
MUTUALLY AUTHENTICATE USER A AND USER B
S771
USER DEVICE A
USER DEVICE B
NO
IS THE MUTUAL AUTHENTICATION COMPLETED SUCCESSFULLY?
S772
YES
S785
EXTRACT A SECURE CONTAINER
S773
INPUT SAMPLING INFORMATION AND A USER ID
S774
EXTRACT AN IDENTIFICATION CERTIFICATE (IDC) LIST FROM THE UCP OR THE PRICE INFORMATION OF THE SECURE CONTAINER
TRANSMIT SAMPLING INFORMATION AND A USER ID TO THE USER DEVICE A
S786
RETRIEVE AN IDENTIFICATION CERTIFICATE (IDC) IDENTIFIER OF THE USER FROM THE IDC LIST ON THE BASIS OF THE USER ID
S775
NO
IS AN IDC IDENTIFIER CORRESPONDING TO THE USER ID FOUND?
S776
YES
EXTRACT THE IDENTIFICATION CERTIFICATE (IDC) ON THE BASIS OF THE IDC IDENTIFIER
S777
COMPARE THE SAMPLING INFORMATION WITH THE TEMPLATE OF THE EXTRACTED IDC
S778
NO
IS THE COMPARISON RESULT CONSISTENT?
S779
YES
S780
TRANSMIT THE UCS (A), THE SECURE CONTAINER, AND THE CONTENT KEY TO THE USER DEVICE B
S781
VERIFY THE UCS (A) AND THE SECURE CONTAINER
S782
ARE THE UCS (A) AND SECURE CONTAINER VALLID?
NO
YES
S783
ERROR
USE THE CONTENT STORED IN THE SECURE CONTAINER
END

FIG. 46

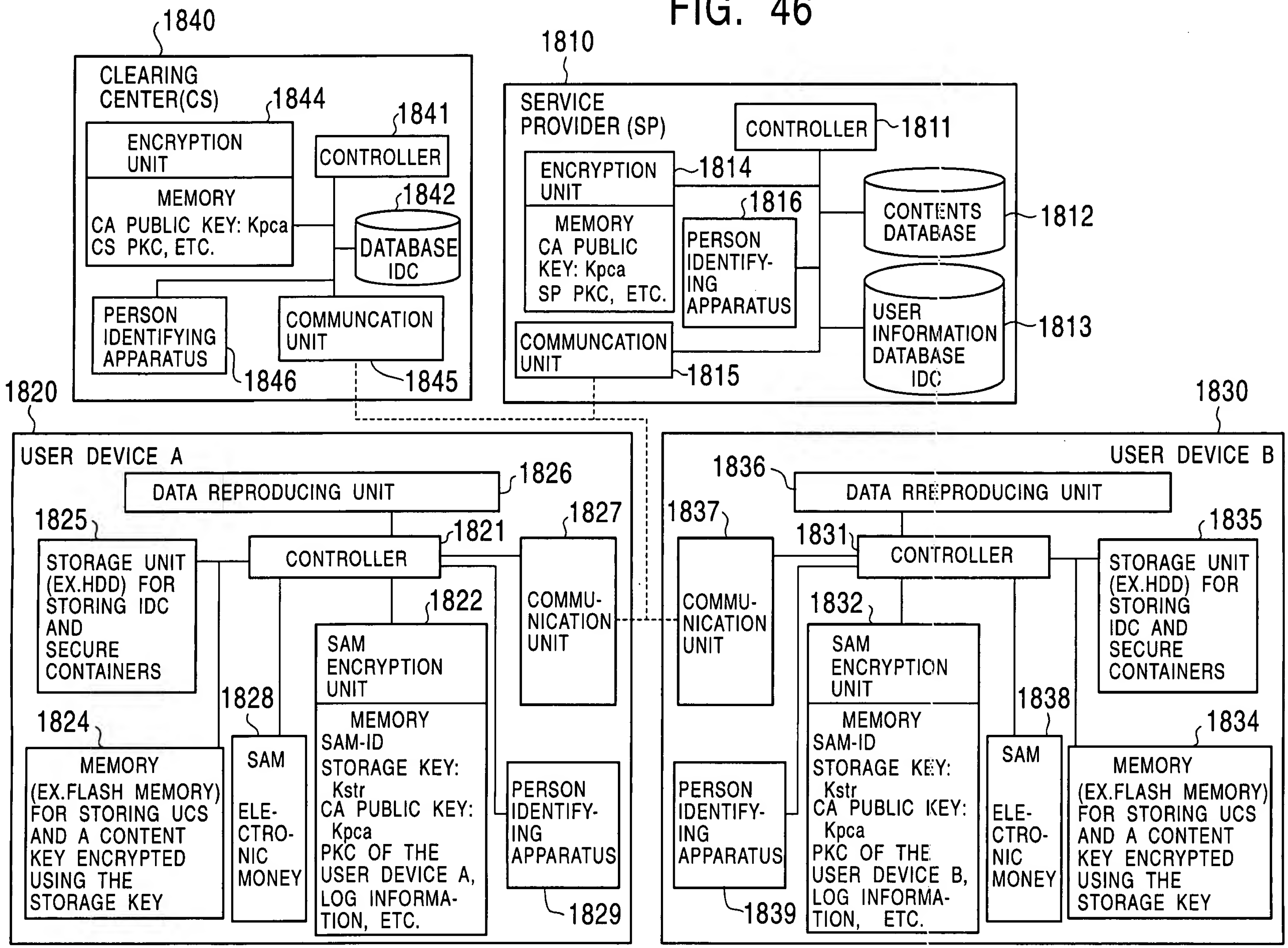

1840
CLEARING CENTER(CS)
1844
ENCRYPTION UNIT
MEMORY
CA PUBLIC KEY: Kpca
CS PKC, ETC.
1841
CONTROLLER
1842
DATABASE
IDC
PERSON IDENTIFYING APPARATUS
1846
COMMUNCATION UNIT
1845
1810
SERVICE PROVIDER (SP)
CONTROLLER
1811
ENCRYPTION UNIT
1814
MEMORY
CA PUBLIC KEY: Kpca
SP PKC, ETC.
1816
PERSON IDENTIFY-ING APPARATUS
CONTENTS DATABASE
1812
USER INFORMATION DATABASE
IDC
1813
COMMUNCATION UNIT
1815
1820
USER DEVICE A
DATA REPRODUCING UNIT
1826
1825
STORAGE UNIT (EX.HDD) FOR STORING IDC AND SECURE CONTAINERS
CONTROLLER
1821
1827
COMMU-NICATION UNIT
1822
SAM ENCRYPTION UNIT
MEMORY
SAM-ID
STORAGE KEY: Kstr
CA PUBLIC KEY: Kpca
PKC OF THE USER DEVICE A, LOG INFORMA-TION, ETC.
1828
SAM
ELE-CTRO-NIC MONEY
1824
MEMORY (EX.FLASH MEMORY) FOR STORING UCS AND A CONTENT KEY ENCRYPTED USING THE STORAGE KEY
PERSON IDENTIFY-ING APPARATUS
1829
1830
USER DEVICE B
1836
DATA RREPRODUCING UNIT
1837
COMMU-NICATION UNIT
1831
CONTROLLER
1835
STORAGE UNIT (EX.HDD) FOR STORING IDC AND SECURE CONTAINERS
1832
SAM ENCRYPTION UNIT
MEMORY
SAM-ID
STORAGE KEY: Kstr
CA PUBLIC KEY: Kpca
PKC OF THE USER DEVICE B, LOG INFORMA-TION, ETC.
1838
SAM
ELE-CTRO-NIC MONEY
1834
MEMORY (EX.FLASH MEMORY) FOR STORING UCS AND A CONTENT KEY ENCRYPTED USING THE STORAGE KEY
PERSON IDENTIFY-ING APPARATUS
1839

FIG. 47A

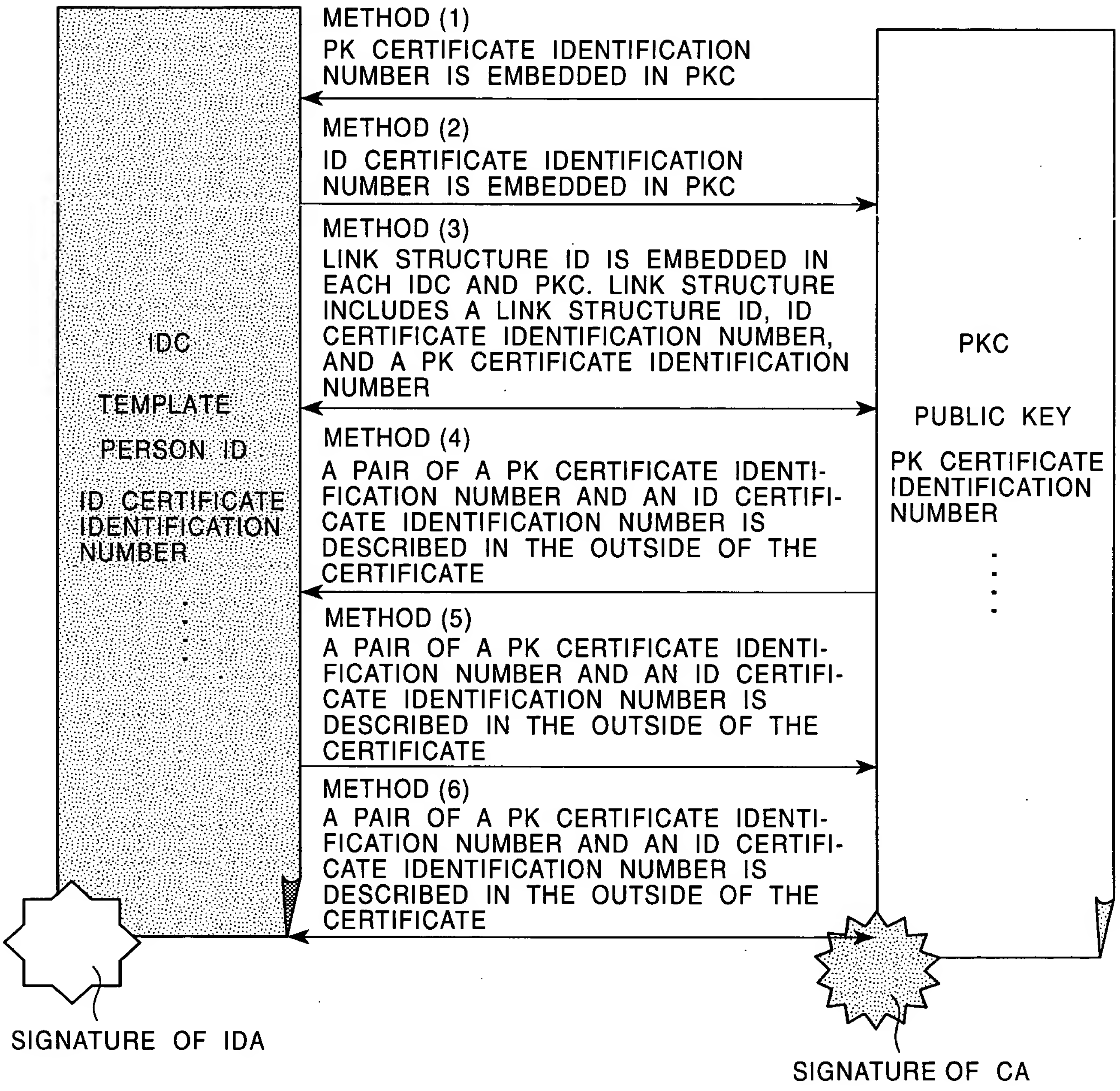

IDC
TEMPLATE
PERSON ID
ID CERTIFICATE IDENTIFICATION NUMBER
METHOD (1)
PK CERTIFICATE IDENTIFICATION NUMBER IS EMBEDDED IN PKC
METHOD (2)
ID CERTIFICATE IDENTIFICATION NUMBER IS EMBEDDED IN PKC
METHOD (3)
LINK STRUCTURE ID IS EMBEDDED IN EACH IDC AND PKC. LINK STRUCTURE INCLUDES A LINK STRUCTURE ID, ID CERTIFICATE IDENTIFICATION NUMBER, AND A PK CERTIFICATE IDENTIFICATION NUMBER
METHOD (4)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
METHOD (5)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
METHOD (6)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
PKC
PUBLIC KEY
PK CERTIFICATE IDENTIFICATION NUMBER
SIGNATURE OF IDA
SIGNATURE OF CA

FIG. 47B

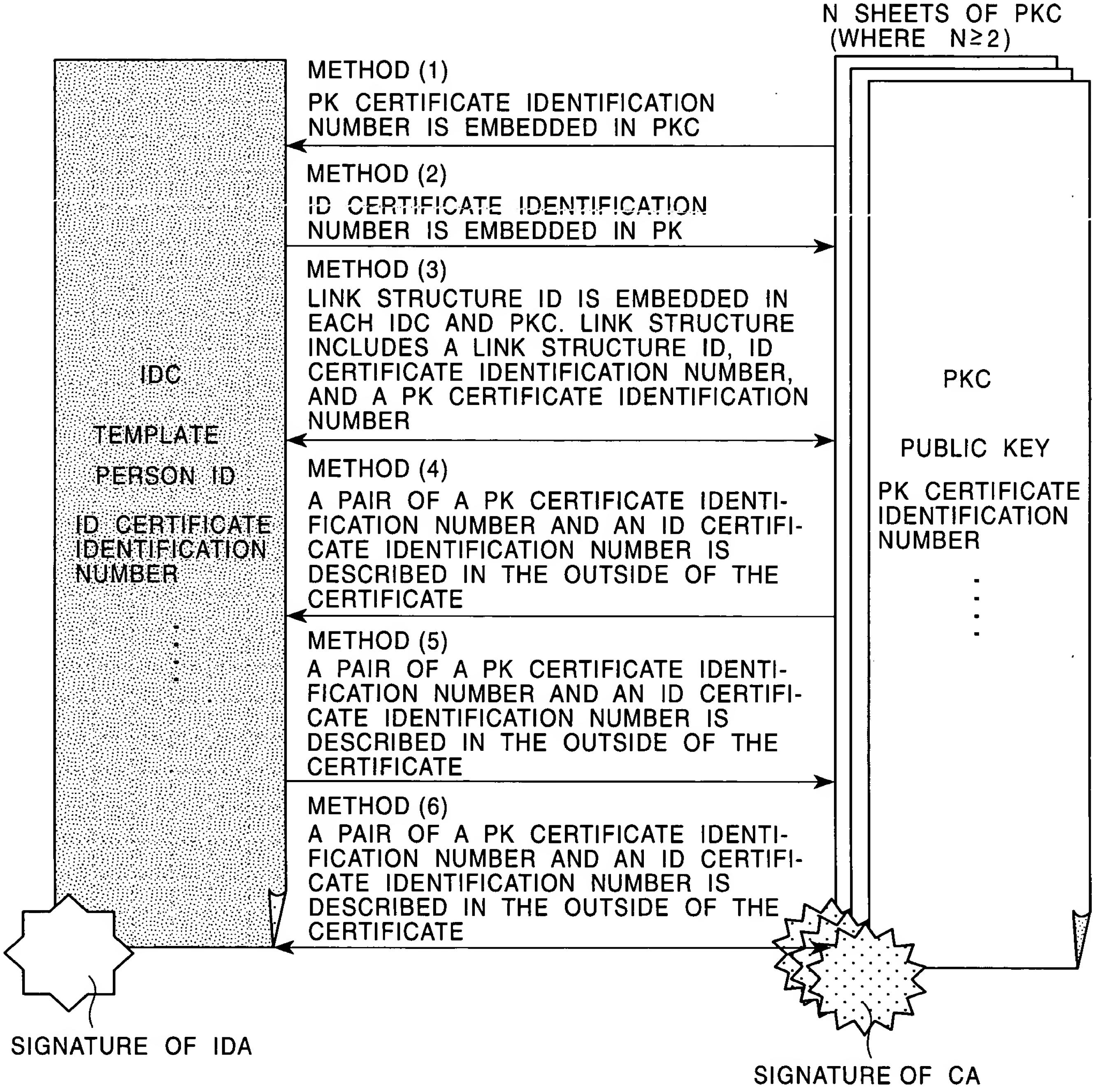

N SHEETS OF PKC (WHERE N≥2)
IDC
TEMPLATE
PERSON ID
ID CERTIFICATE IDENTIFICATION NUMBER
METHOD (1)
PK CERTIFICATE IDENTIFICATION NUMBER IS EMBEDDED IN PKC
METHOD (2)
ID CERTIFICATE IDENTIFICATION NUMBER IS EMBEDDED IN PK
METHOD (3)
LINK STRUCTURE ID IS EMBEDDED IN EACH IDC AND PKC. LINK STRUCTURE INCLUDES A LINK STRUCTURE ID, ID CERTIFICATE IDENTIFICATION NUMBER, AND A PK CERTIFICATE IDENTIFICATION NUMBER
METHOD (4)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
METHOD (5)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
METHOD (6)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
PKC
PUBLIC KEY
PK CERTIFICATE IDENTIFICATION NUMBER
SIGNATURE OF IDA
SIGNATURE OF CA

FIG. 48A

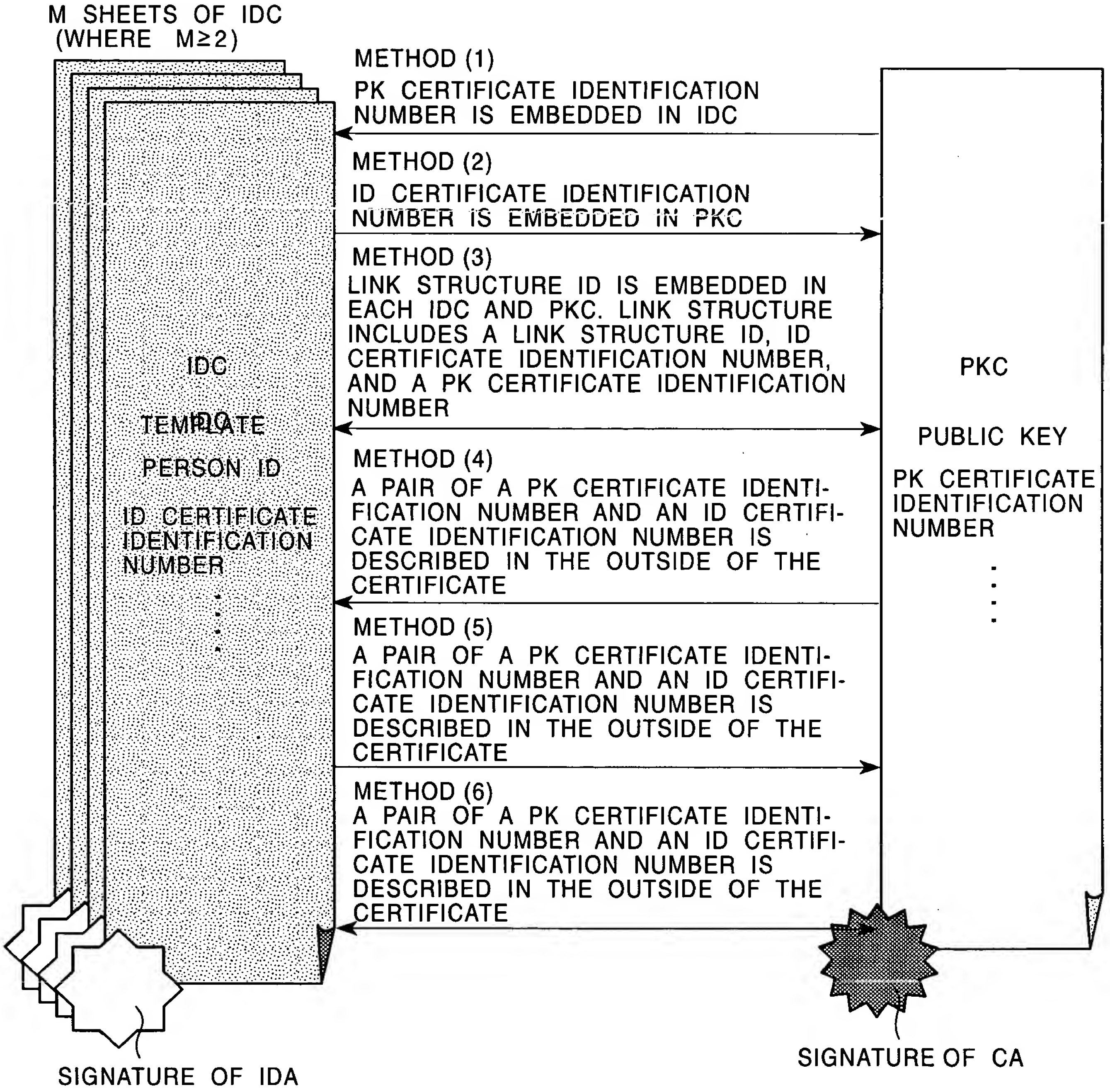

M SHEETS OF IDC
(WHERE M≥2)
METHOD (1)
PK CERTIFICATE IDENTIFICATION NUMBER IS EMBEDDED IN IDC
METHOD (2)
ID CERTIFICATE IDENTIFICATION NUMBER IS EMBEDDED IN PKC
METHOD (3)
LINK STRUCTURE ID IS EMBEDDED IN EACH IDC AND PKC. LINK STRUCTURE INCLUDES A LINK STRUCTURE ID, ID CERTIFICATE IDENTIFICATION NUMBER, AND A PK CERTIFICATE IDENTIFICATION NUMBER
METHOD (4)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
METHOD (5)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
METHOD (6)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
IDC
TEMPLATE
IDO
PERSON ID
ID CERTIFICATE IDENTIFICATION NUMBER
PKC
PUBLIC KEY
PK CERTIFICATE IDENTIFICATION NUMBER
SIGNATURE OF IDA
SIGNATURE OF CA

FIG. 48B

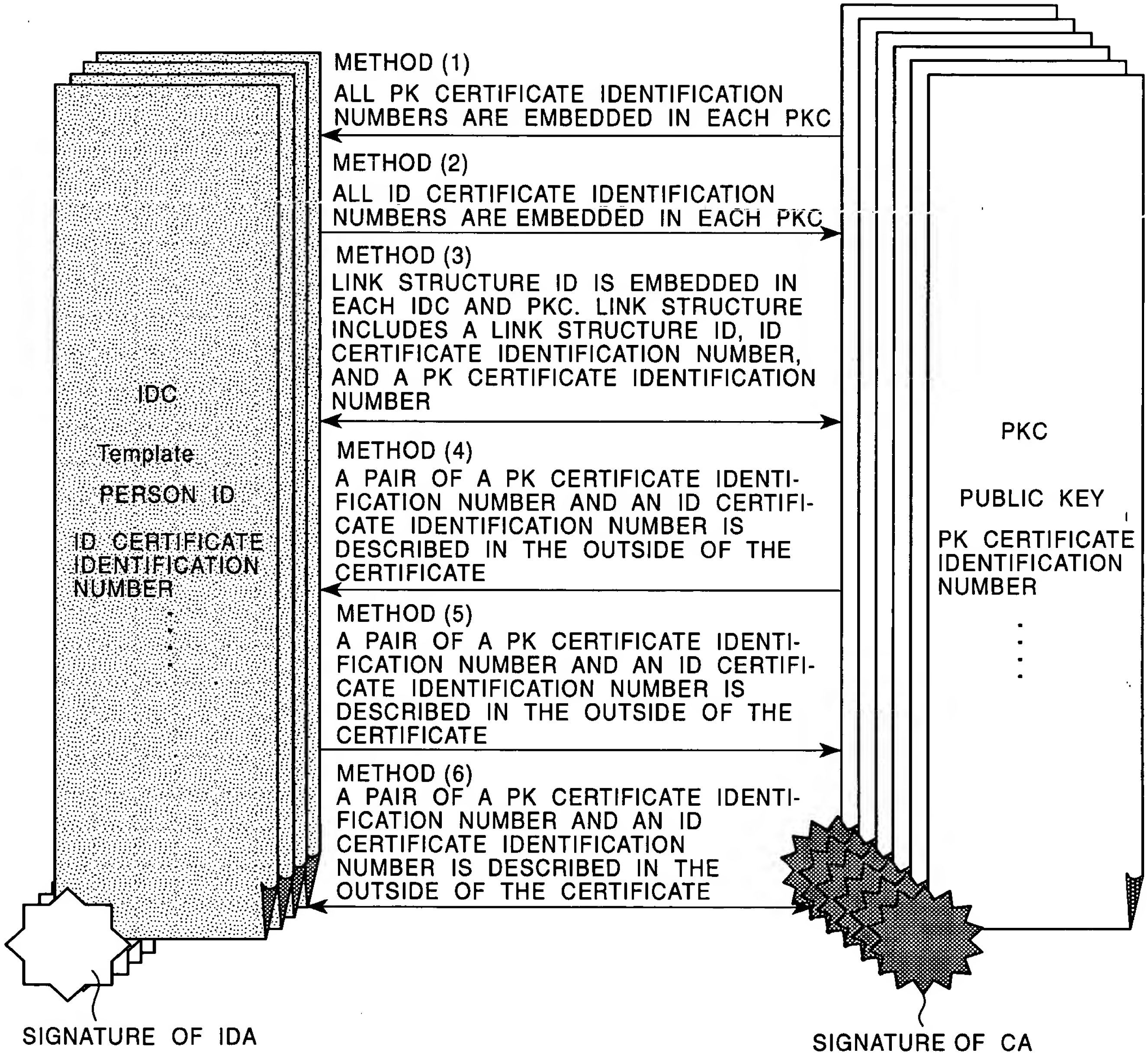

METHOD (1)
ALL PK CERTIFICATE IDENTIFICATION NUMBERS ARE EMBEDDED IN EACH PKC
METHOD (2)
ALL ID CERTIFICATE IDENTIFICATION NUMBERS ARE EMBEDDED IN EACH PKC
METHOD (3)
LINK STRUCTURE ID IS EMBEDDED IN EACH IDC AND PKC. LINK STRUCTURE INCLUDES A LINK STRUCTURE ID, ID CERTIFICATE IDENTIFICATION NUMBER, AND A PK CERTIFICATE IDENTIFICATION NUMBER
METHOD (4)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
METHOD (5)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
METHOD (6)
A PAIR OF A PK CERTIFICATE IDENTIFICATION NUMBER AND AN ID CERTIFICATE IDENTIFICATION NUMBER IS DESCRIBED IN THE OUTSIDE OF THE CERTIFICATE
IDC
Template
PERSON ID
ID CERTIFICATE IDENTIFICATION NUMBER
PKC
PUBLIC KEY
PK CERTIFICATE IDENTIFICATION NUMBER
SIGNATURE OF IDA
SIGNATURE OF CA

FIG. 49A

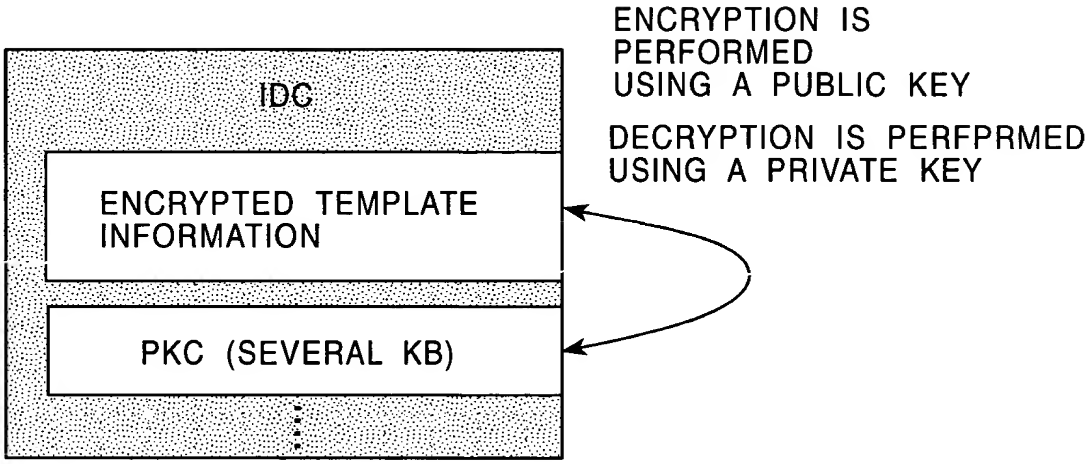

ENCRYPTION IS PERFORMED USING A PUBLIC KEY
DECRYPTION IS PERFPRMED USING A PRIVATE KEY
IDC
ENCRYPTED TEMPLATE INFORMATION
PKC (SEVERAL KB)

FIG. 49B

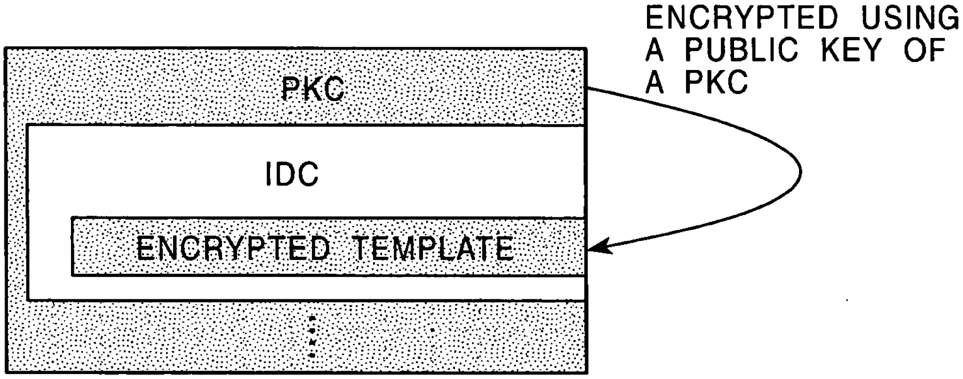


FIG. 50A

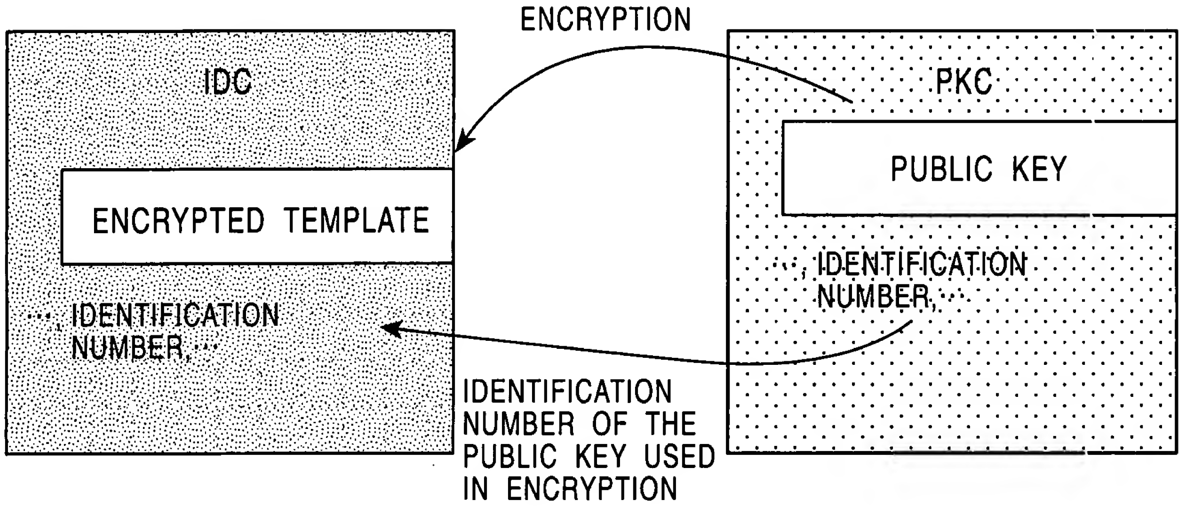

ENCRYPTION
IDC
ENCRYPTED TEMPLATE
…, IDENTIFICATION NUMBER, …
PKC
PUBLIC KEY
…, IDENTIFICATION NUMBER, …
IDENTIFICATION NUMBER OF THE PUBLIC KEY USED IN ENCRYPTION

FIG. 50B

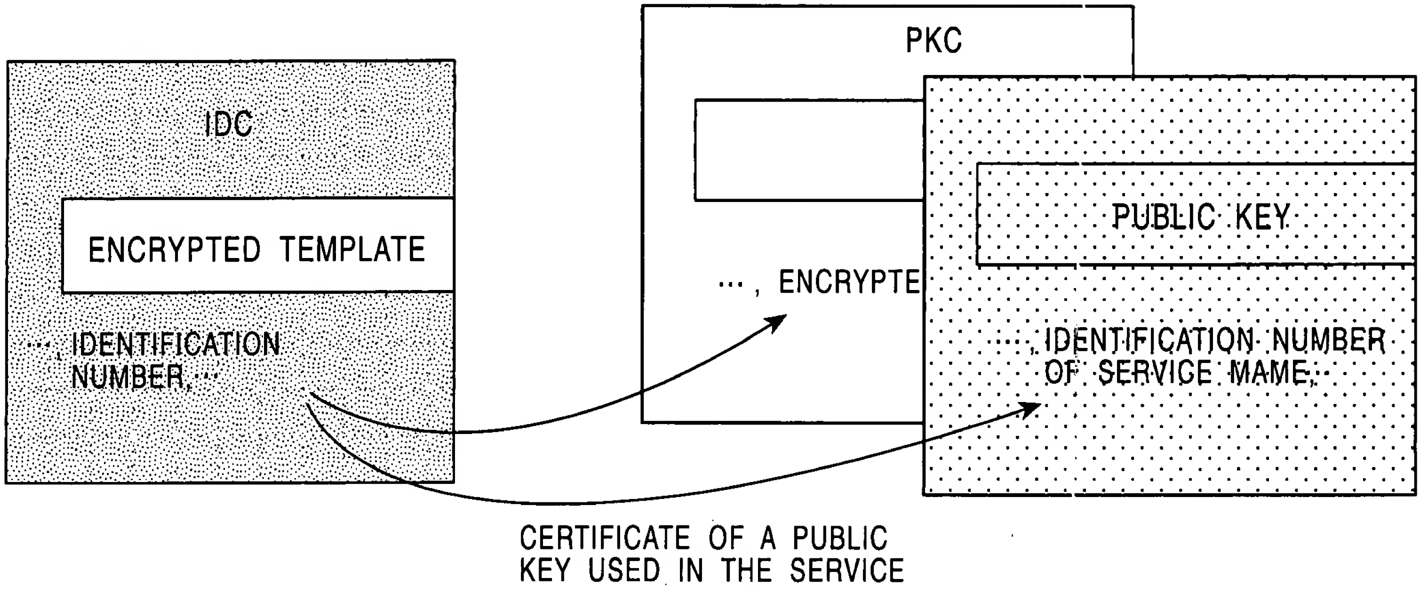

IDC
ENCRYPTED TEMPLATE
…, IDENTIFICATION NUMBER, …
PKC
…, ENCRYPTE
PUBLIC KEY
…, IDENTIFICATION NUMBER OF SERVICE MAME, …
CERTIFICATE OF A PUBLIC KEY USED IN THE SERVICE

FIG. 51A

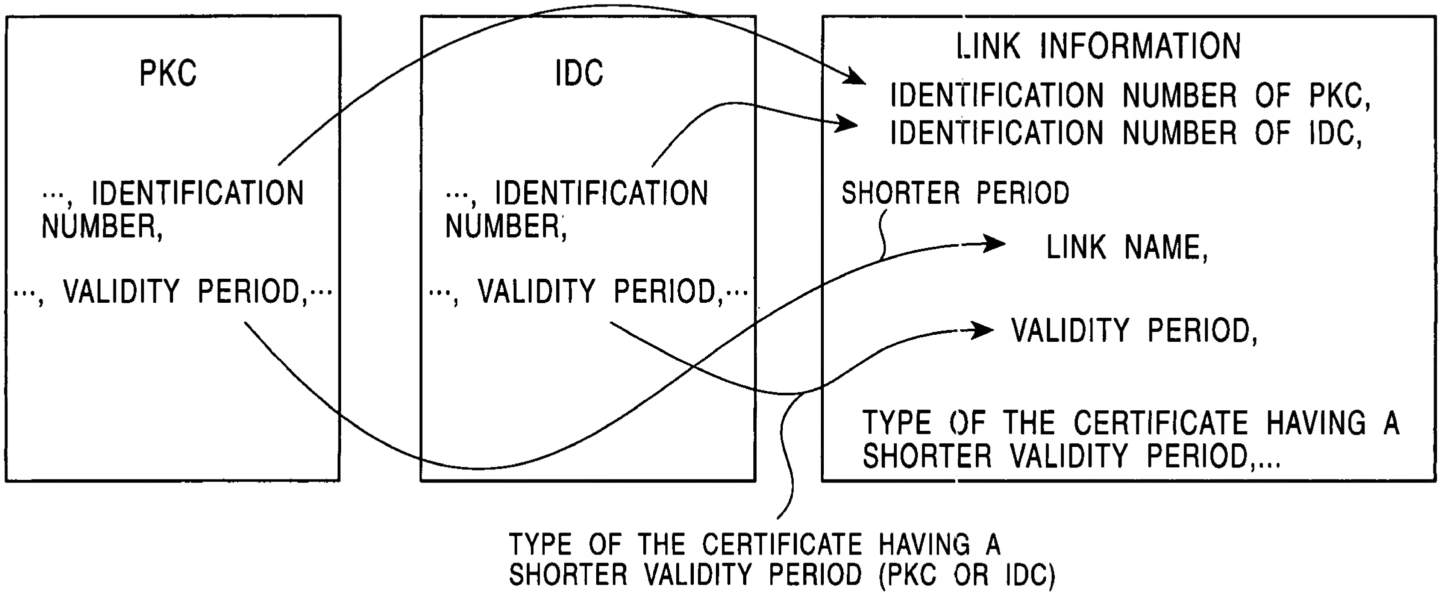

PKC
…, IDENTIFICATION NUMBER,
…, VALIDITY PERIOD,…
IDC
…, IDENTIFICATION NUMBER;
…, VALIDITY PERIOD,…
LINK INFORMATION
IDENTIFICATION NUMBER OF PKC,
IDENTIFICATION NUMBER OF IDC,
SHORTER PERIOD
LINK NAME,
VALIDITY PERIOD,
TYPE OF THE CERTIFICATE HAVING A SHORTER VALIDITY PERIOD,...
TYPE OF THE CERTIFICATE HAVING A SHORTER VALIDITY PERIOD (PKC OR IDC)

FIG. 51B

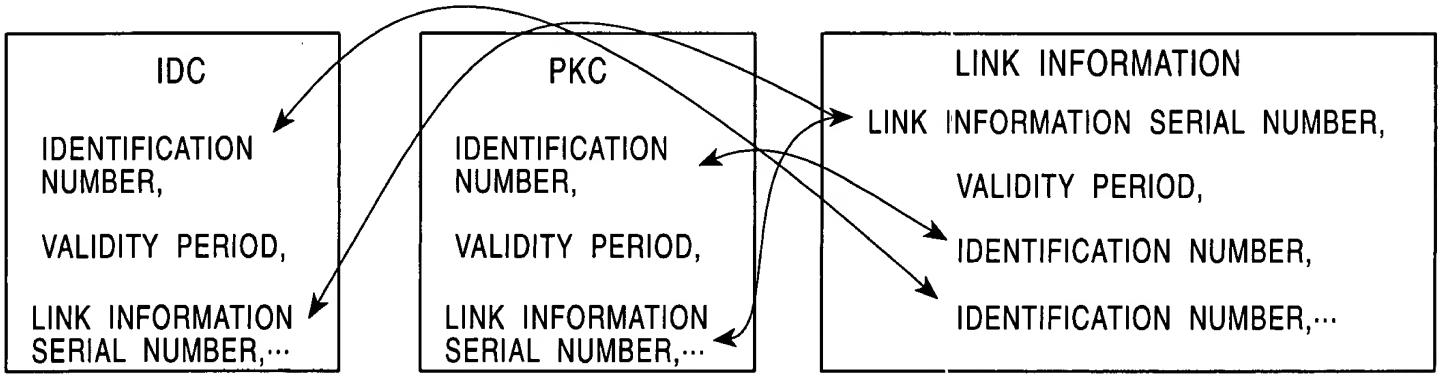


FIG. 52A

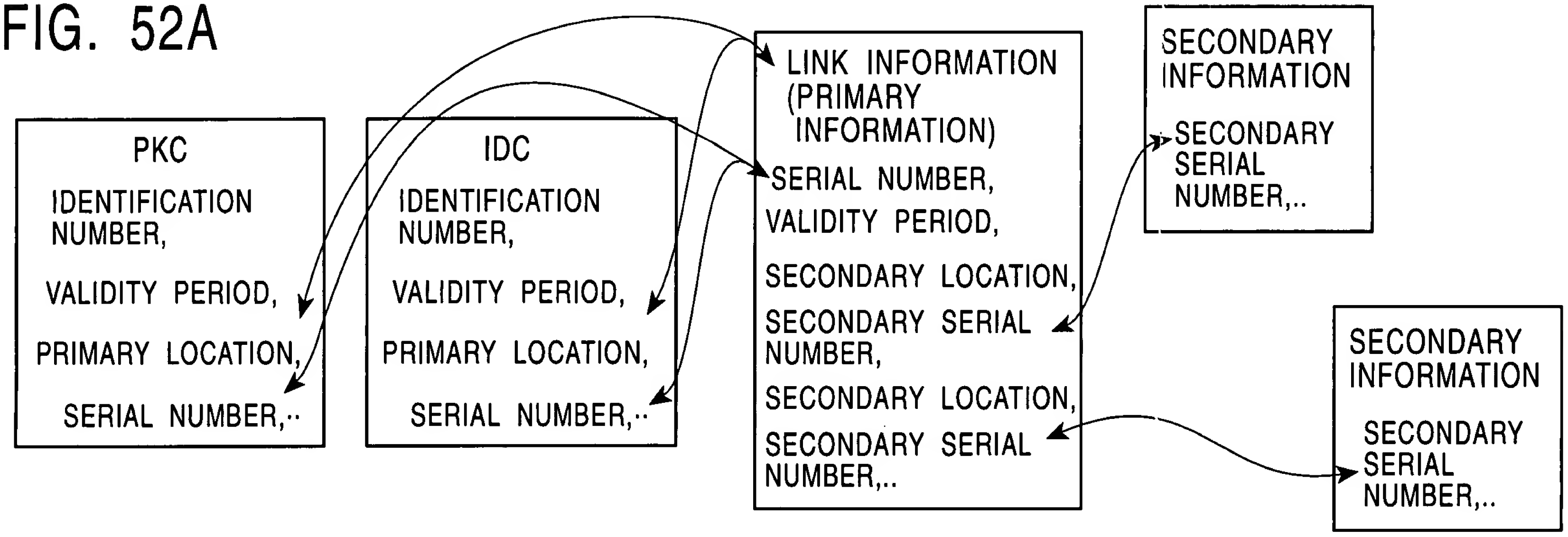


FIG. 52B

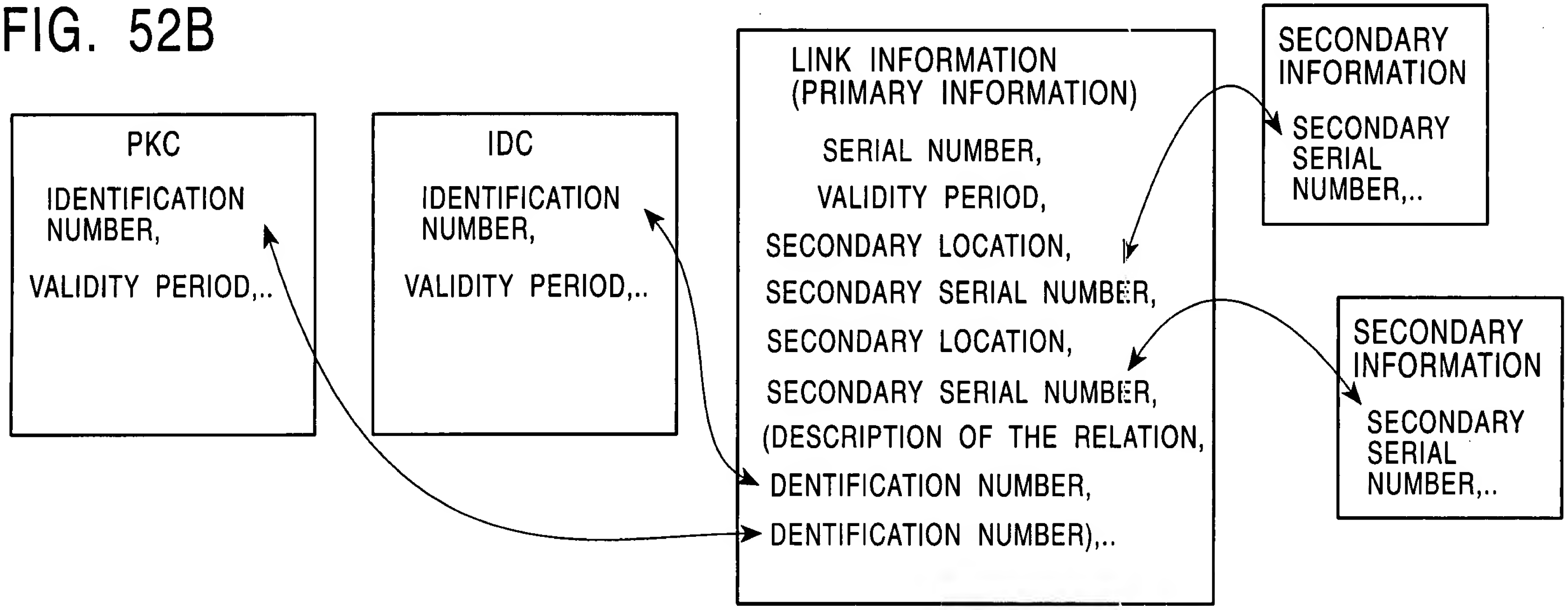


FIG. 53

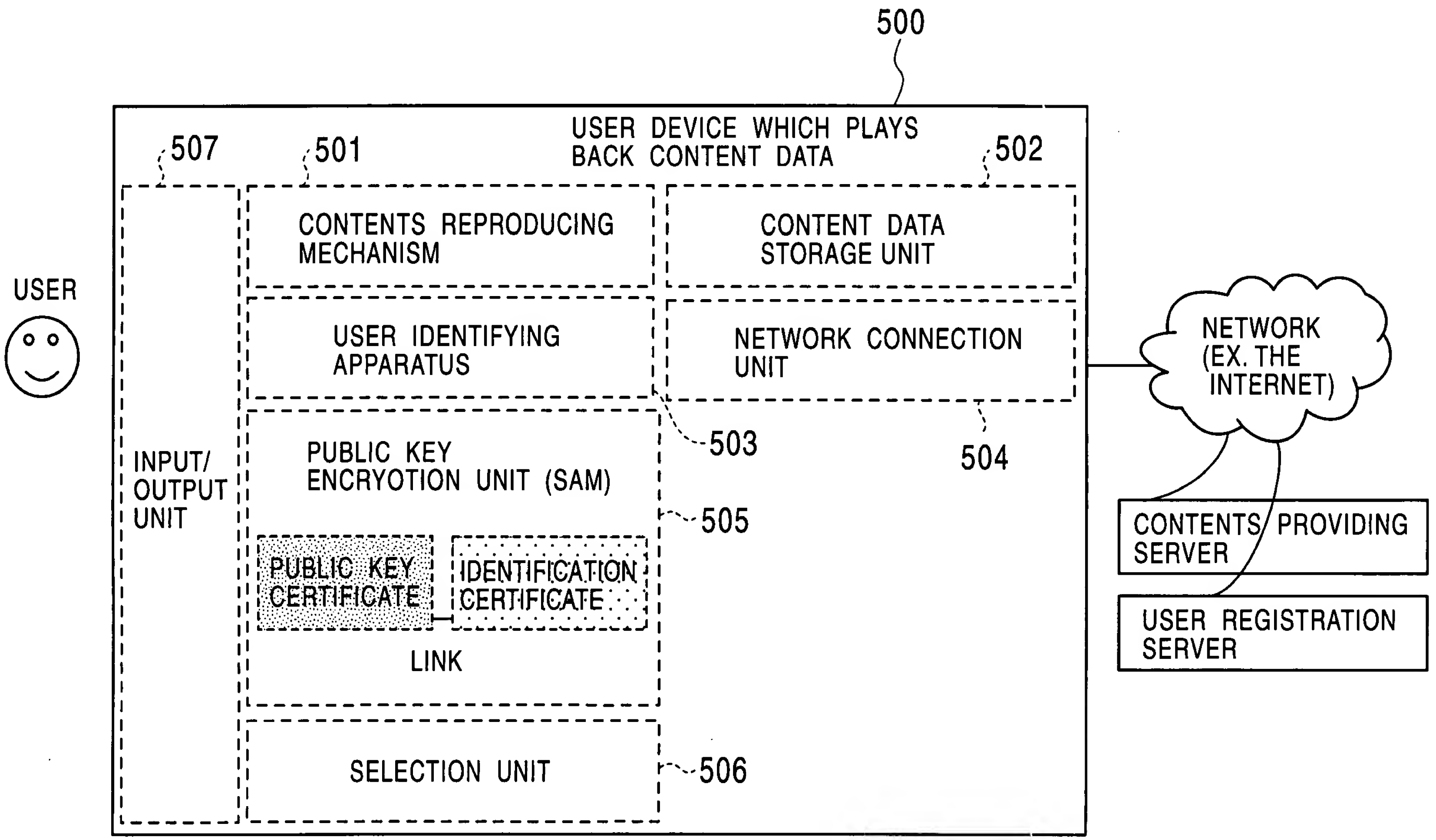

500
USER DEVICE WHICH PLAYS BACK CONTENT DATA
507
501
502
USER
CONTENTS REPRODUCING MECHANISM
CONTENT DATA STORAGE UNIT
USER IDENTIFYING APPARATUS
NETWORK CONNECTION UNIT
503
504
INPUT/ OUTPUT UNIT
PUBLIC KEY ENCRYOTION UNIT (SAM)
505
PUBLIC KEY CERTIFICATE
IDENTIFICATION CERTIFICATE
LINK
SELECTION UNIT
506
NETWORK (EX. THE INTERNET)
CONTENTS PROVIDING SERVER
USER REGISTRATION SERVER

FIG. 54

PRECONDITIONS:

- IDC AND PKC HAVE BEEN ACQUIRED
- USER REGISTRATION IN THE CONTENTS PROVIDING SERVER HAS BEEN PERFORMED

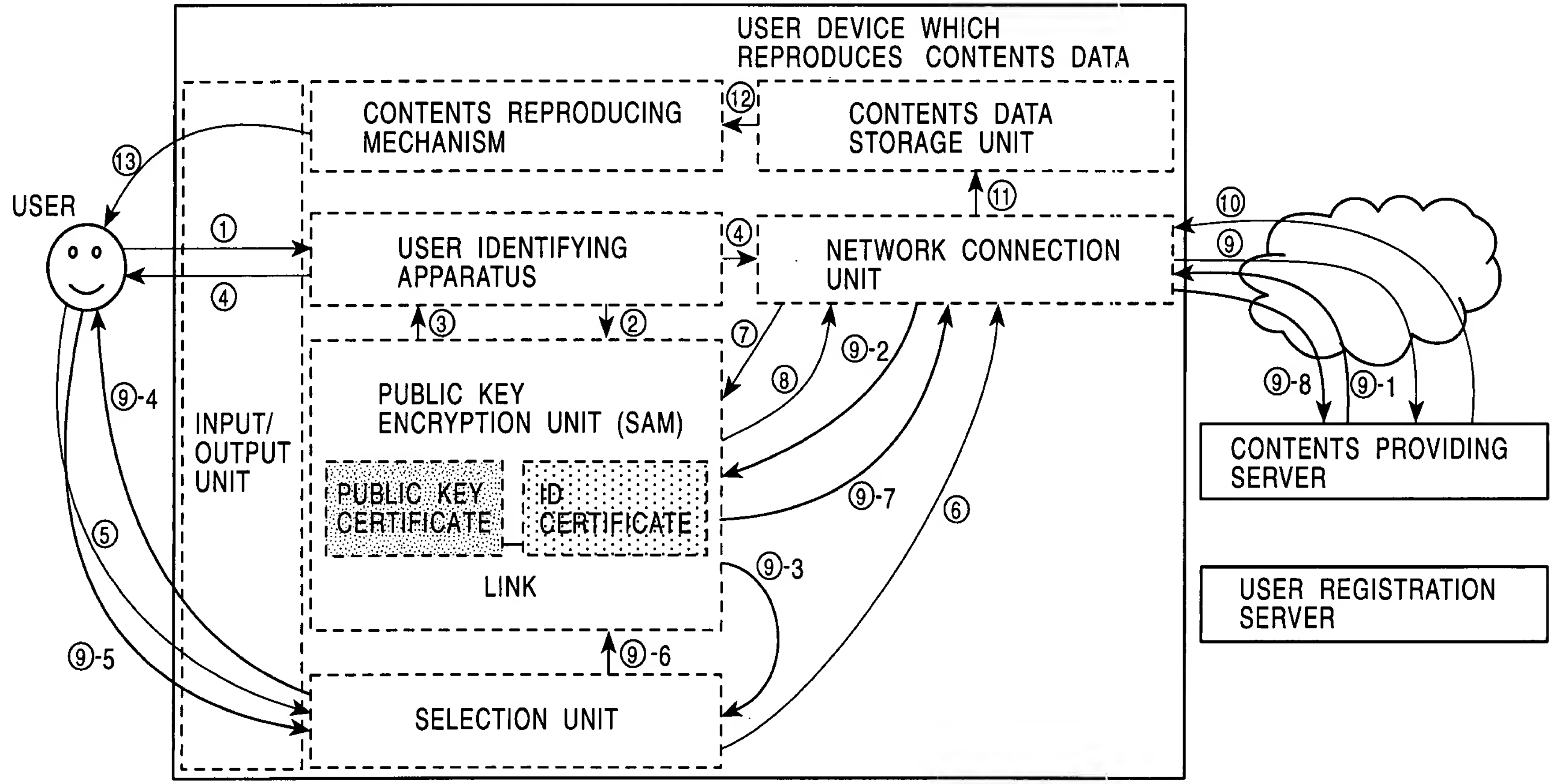

USER
USER DEVICE WHICH REPRODUCES CONTENTS DATA
INPUT/ OUTPUT UNIT
CONTENTS REPRODUCING MECHANISM
CONTENTS DATA STORAGE UNIT
USER IDENTIFYING APPARATUS
NETWORK CONNECTION UNIT
PUBLIC KEY ENCRYPTION UNIT (SAM)
PUBLIC KEY CERTIFICATE
ID CERTIFICATE
LINK
SELECTION UNIT
CONTENTS PROVIDING SERVER
USER REGISTRATION SERVER
①
②
③
④
④
⑤
⑥
⑦
⑧
⑨
⑨-1
⑨-2
⑨-3
⑨-4
⑨-5
⑨-6
⑨-7
⑨-8
⑩
⑪
⑫
⑬

FIG. 55

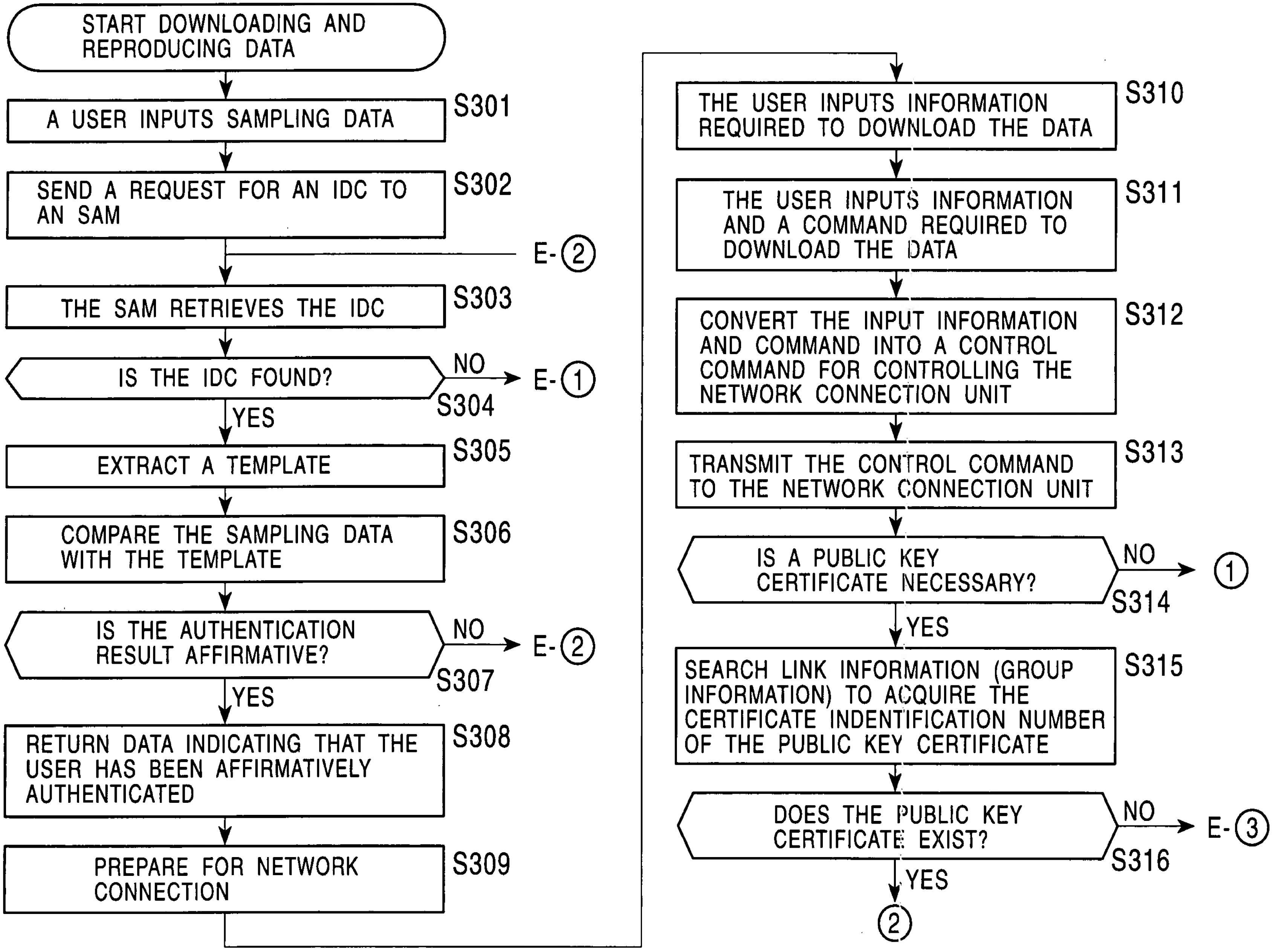

START DOWNLOADING AND REPRODUCING DATA
A USER INPUTS SAMPLING DATA
S301
SEND A REQUEST FOR AN IDC TO AN SAM
S302
E-②
THE SAM RETRIEVES THE IDC
S303
IS THE IDC FOUND?
S304
NO
E-①
YES
EXTRACT A TEMPLATE
S305
COMPARE THE SAMPLING DATA WITH THE TEMPLATE
S306
IS THE AUTHENTICATION RESULT AFFIRMATIVE?
S307
NO
E-②
YES
RETURN DATA INDICATING THAT THE USER HAS BEEN AFFIRMATIVELY AUTHENTICATED
S308
PREPARE FOR NETWORK CONNECTION
S309
THE USER INPUTS INFORMATION REQUIRED TO DOWNLOAD THE DATA
S310
THE USER INPUTS INFORMATION AND A COMMAND REQUIRED TO DOWNLOAD THE DATA
S311
CONVERT THE INPUT INFORMATION AND COMMAND INTO A CONTROL COMMAND FOR CONTROLLING THE NETWORK CONNECTION UNIT
S312
TRANSMIT THE CONTROL COMMAND TO THE NETWORK CONNECTION UNIT
S313
IS A PUBLIC KEY CERTIFICATE NECESSARY?
S314
NO
①
YES
SEARCH LINK INFORMATION (GROUP INFORMATION) TO ACQUIRE THE CERTIFICATE INDENTIFICATION NUMBER OF THE PUBLIC KEY CERTIFICATE
S315
DOES THE PUBLIC KEY CERTIFICATE EXIST?
S316
NO
E-③
YES
②

FIG. 56

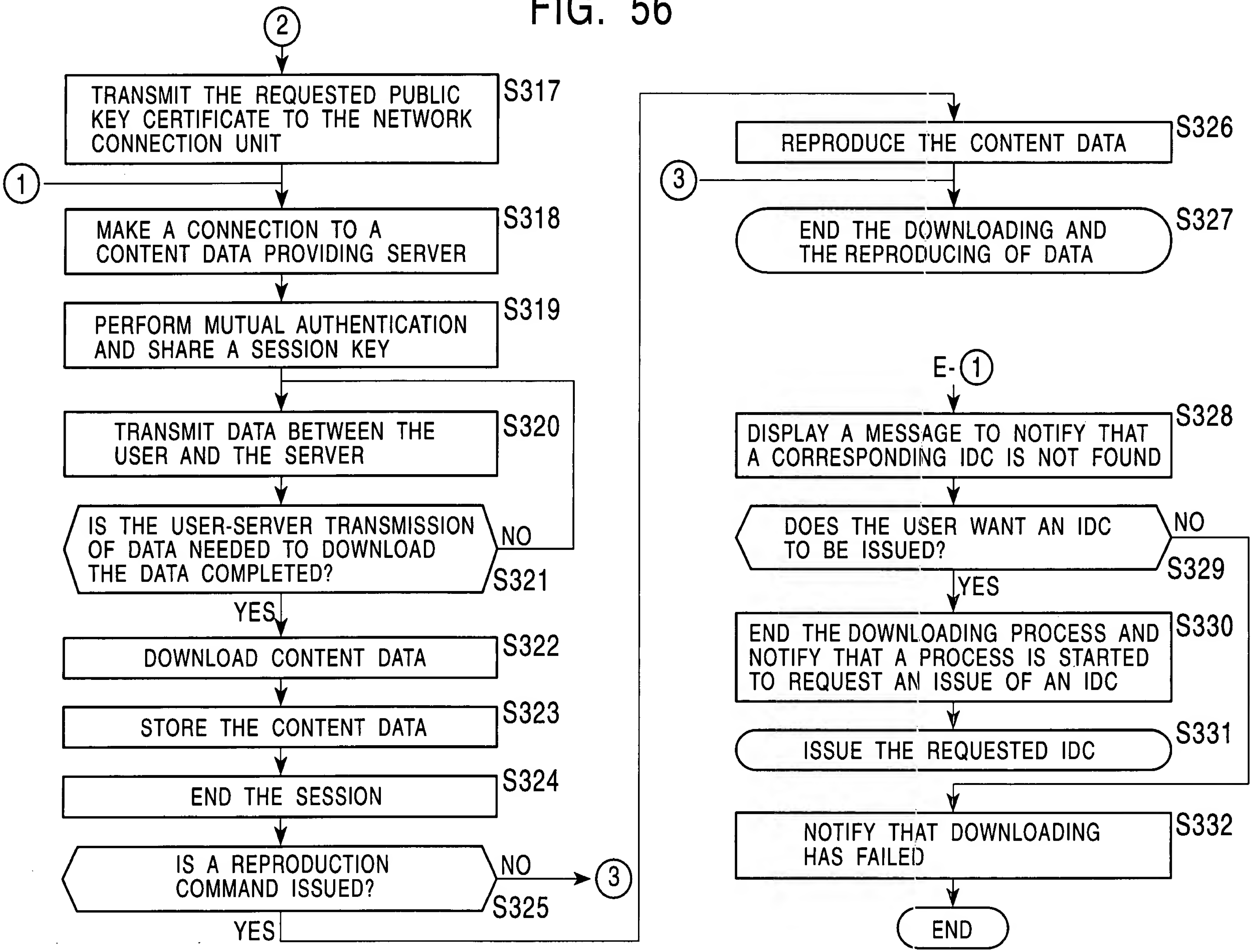

2
TRANSMIT THE REQUESTED PUBLIC KEY CERTIFICATE TO THE NETWORK CONNECTION UNIT
S317
1
MAKE A CONNECTION TO A CONTENT DATA PROVIDING SERVER
S318
PERFORM MUTUAL AUTHENTICATION AND SHARE A SESSION KEY
S319
TRANSMIT DATA BETWEEN THE USER AND THE SERVER
S320
IS THE USER-SERVER TRANSMISSION OF DATA NEEDED TO DOWNLOAD THE DATA COMPLETED?
NO
S321
YES
DOWNLOAD CONTENT DATA
S322
STORE THE CONTENT DATA
S323
END THE SESSION
S324
IS A REPRODUCTION COMMAND ISSUED?
NO
3
S325
YES
REPRODUCE THE CONTENT DATA
S326
3
END THE DOWNLOADING AND THE REPRODUCING OF DATA
S327
E-1
DISPLAY A MESSAGE TO NOTIFY THAT A CORRESPONDING IDC IS NOT FOUND
S328
DOES THE USER WANT AN IDC TO BE ISSUED?
NO
S329
YES
END THE DOWNLOADING PROCESS AND NOTIFY THAT A PROCESS IS STARTED TO REQUEST AN ISSUE OF AN IDC
S330
ISSUE THE REQUESTED IDC
S331
NOTIFY THAT DOWNLOADING HAS FAILED
S332
END

FIG. 57

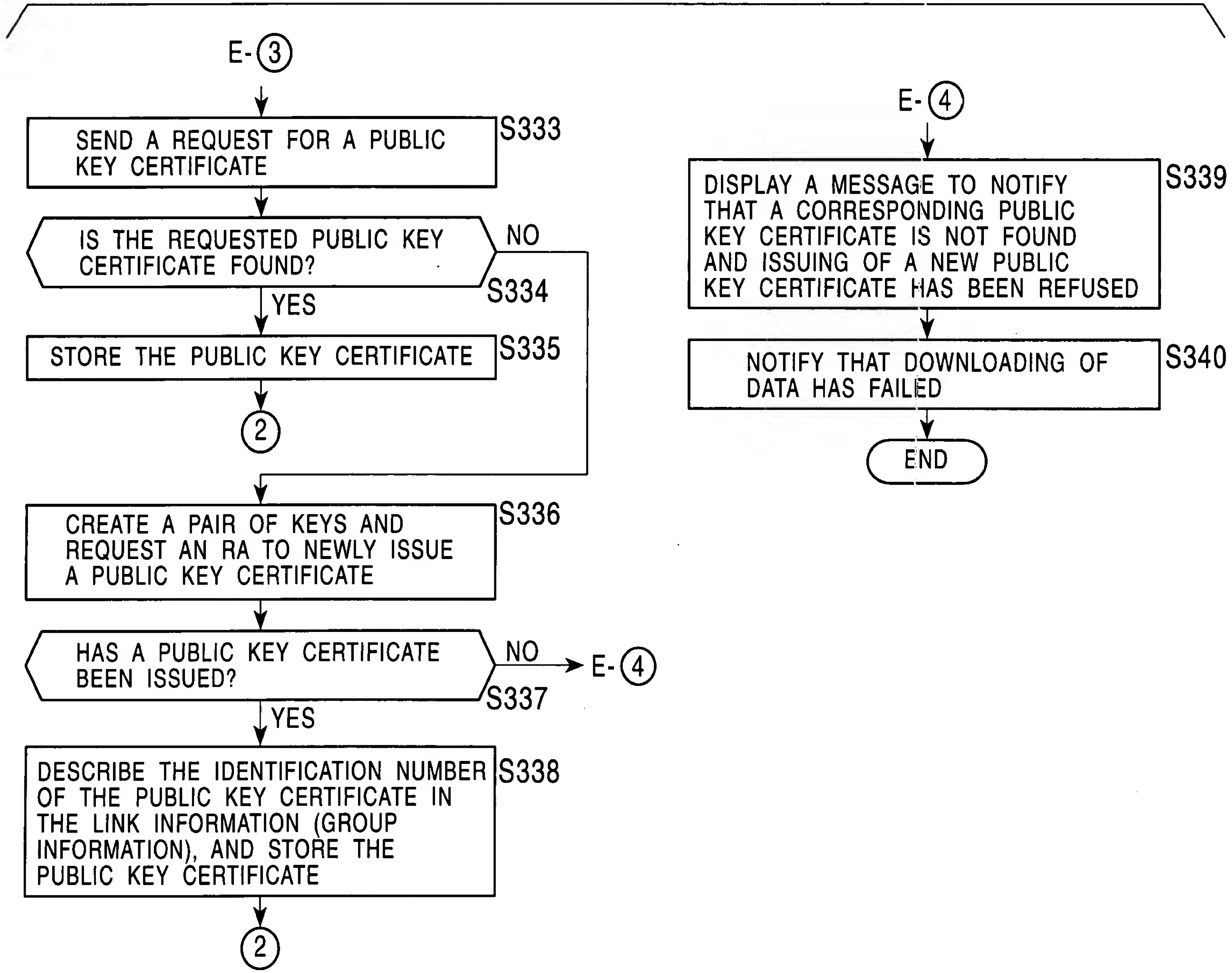

E-③
SEND A REQUEST FOR A PUBLIC KEY CERTIFICATE
S333
IS THE REQUESTED PUBLIC KEY CERTIFICATE FOUND?
S334
NO
YES
STORE THE PUBLIC KEY CERTIFICATE
S335
②
CREATE A PAIR OF KEYS AND REQUEST AN RA TO NEWLY ISSUE A PUBLIC KEY CERTIFICATE
S336
HAS A PUBLIC KEY CERTIFICATE BEEN ISSUED?
S337
NO
E-④
YES
DESCRIBE THE IDENTIFICATION NUMBER OF THE PUBLIC KEY CERTIFICATE IN THE LINK INFORMATION (GROUP INFORMATION), AND STORE THE PUBLIC KEY CERTIFICATE
S338
②
E-④
DISPLAY A MESSAGE TO NOTIFY THAT A CORRESPONDING PUBLIC KEY CERTIFICATE IS NOT FOUND AND ISSUING OF A NEW PUBLIC KEY CERTIFICATE HAS BEEN REFUSED
S339
NOTIFY THAT DOWNLOADING OF DATA HAS FAILED
S340
END

FIG. 58

PRECONDITION:

- IDC AND PKC HAVE BEEN ACQUIRED

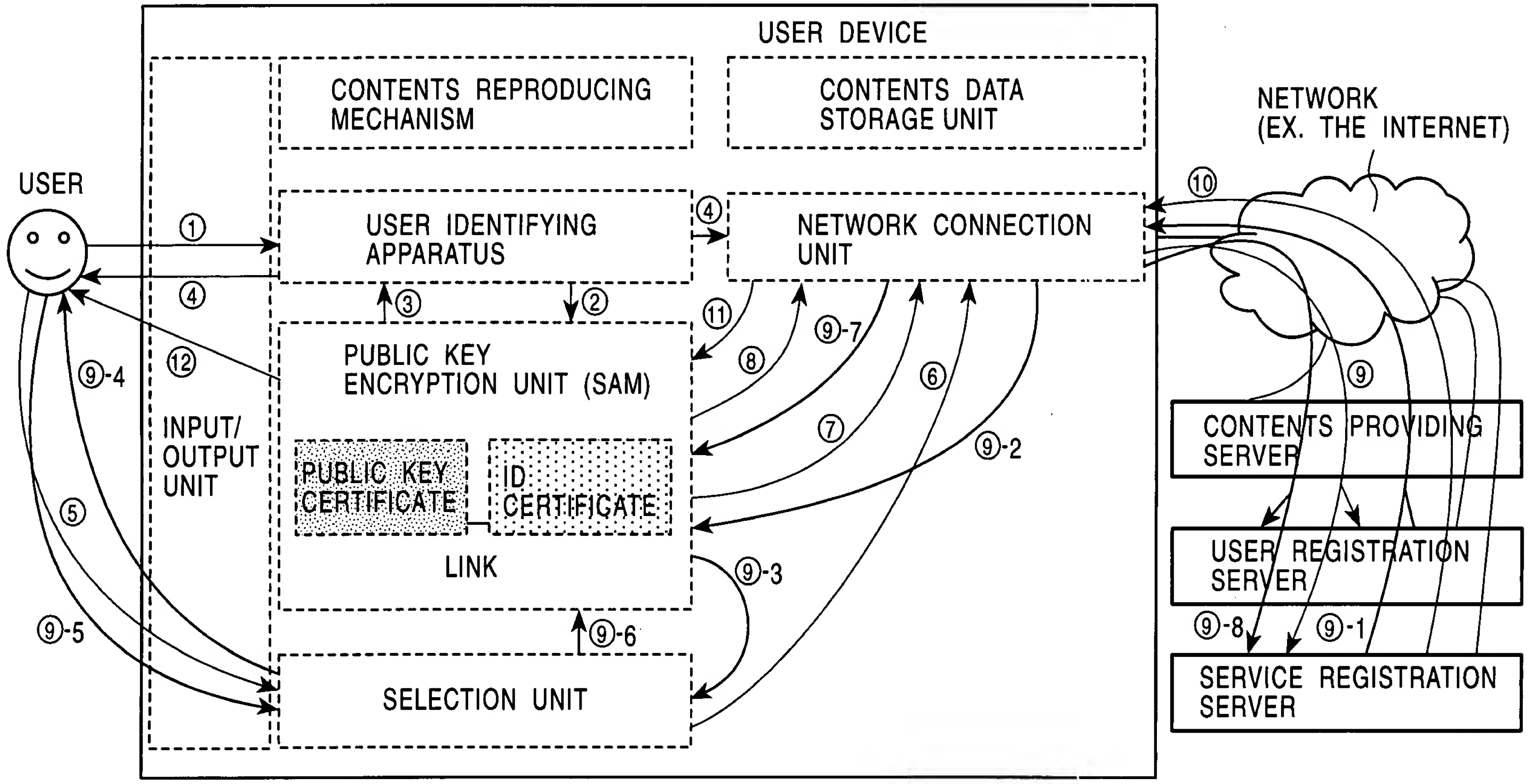

USER
USER DEVICE
CONTENTS REPRODUCING MECHANISM
CONTENTS DATA STORAGE UNIT
USER IDENTIFYING APPARATUS
NETWORK CONNECTION UNIT
PUBLIC KEY ENCRYPTION UNIT (SAM)
PUBLIC KEY CERTIFICATE
ID CERTIFICATE
LINK
SELECTION UNIT
INPUT/ OUTPUT UNIT
NETWORK (EX. THE INTERNET)
CONTENTS PROVIDING SERVER
USER REGISTRATION SERVER
SERVICE REGISTRATION SERVER
①
②
③
④
④
⑤
⑥
⑦
⑧
⑨
⑨-1
⑨-2
⑨-3
⑨-4
⑨-5
⑨-6
⑨-7
⑨-8
⑩
⑪
⑫

FIG. 59

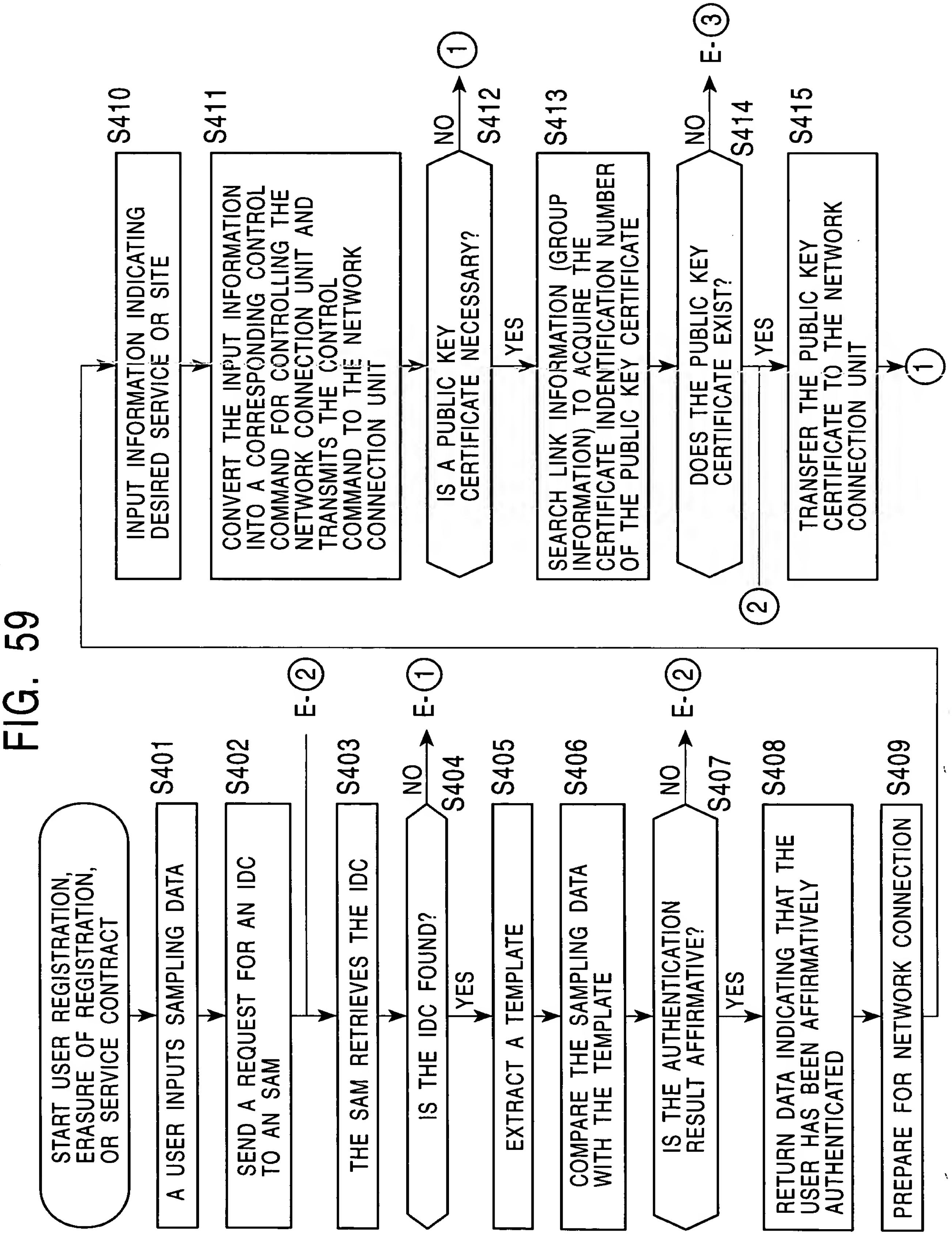

START USER REGISTRATION, ERASURE OF REGISTRATION, OR SERVICE CONTRACT
S401
A USER INPUTS SAMPLING DATA
S402
SEND A REQUEST FOR AN IDC TO AN SAM
E-2
S403
THE SAM RETRIEVES THE IDC
S404
IS THE IDC FOUND?
NO
E-1
YES
S405
EXTRACT A TEMPLATE
S406
COMPARE THE SAMPLING DATA WITH THE TEMPLATE
S407
IS THE AUTHENTICATION RESULT AFFIRMATIVE?
NO
E-2
YES
S408
RETURN DATA INDICATING THAT THE USER HAS BEEN AFFIRMATIVELY AUTHENTICATED
S409
PREPARE FOR NETWORK CONNECTION
S410
INPUT INFORMATION INDICATING DESIRED SERVICE OR SITE
S411
CONVERT THE INPUT INFORMATION INTO A CORRESPONDING CONTROL COMMAND FOR CONTROLLING THE NETWORK CONNECTION UNIT AND TRANSMITS THE CONTROL COMMAND TO THE NETWORK CONNECTION UNIT
S412
IS A PUBLIC KEY CERTIFICATE NECESSARY?
NO
1
YES
S413
SEARCH LINK INFORMATION (GROUP INFORMATION) TO ACQUIRE THE CERTIFICATE INDENTIFICATION NUMBER OF THE PUBLIC KEY CERTIFICATE
S414
DOES THE PUBLIC KEY CERTIFICATE EXIST?
NO
E-3
YES
2
S415
TRANSFER THE PUBLIC KEY CERTIFICATE TO THE NETWORK CONNECTION UNIT
1

FIG. 60

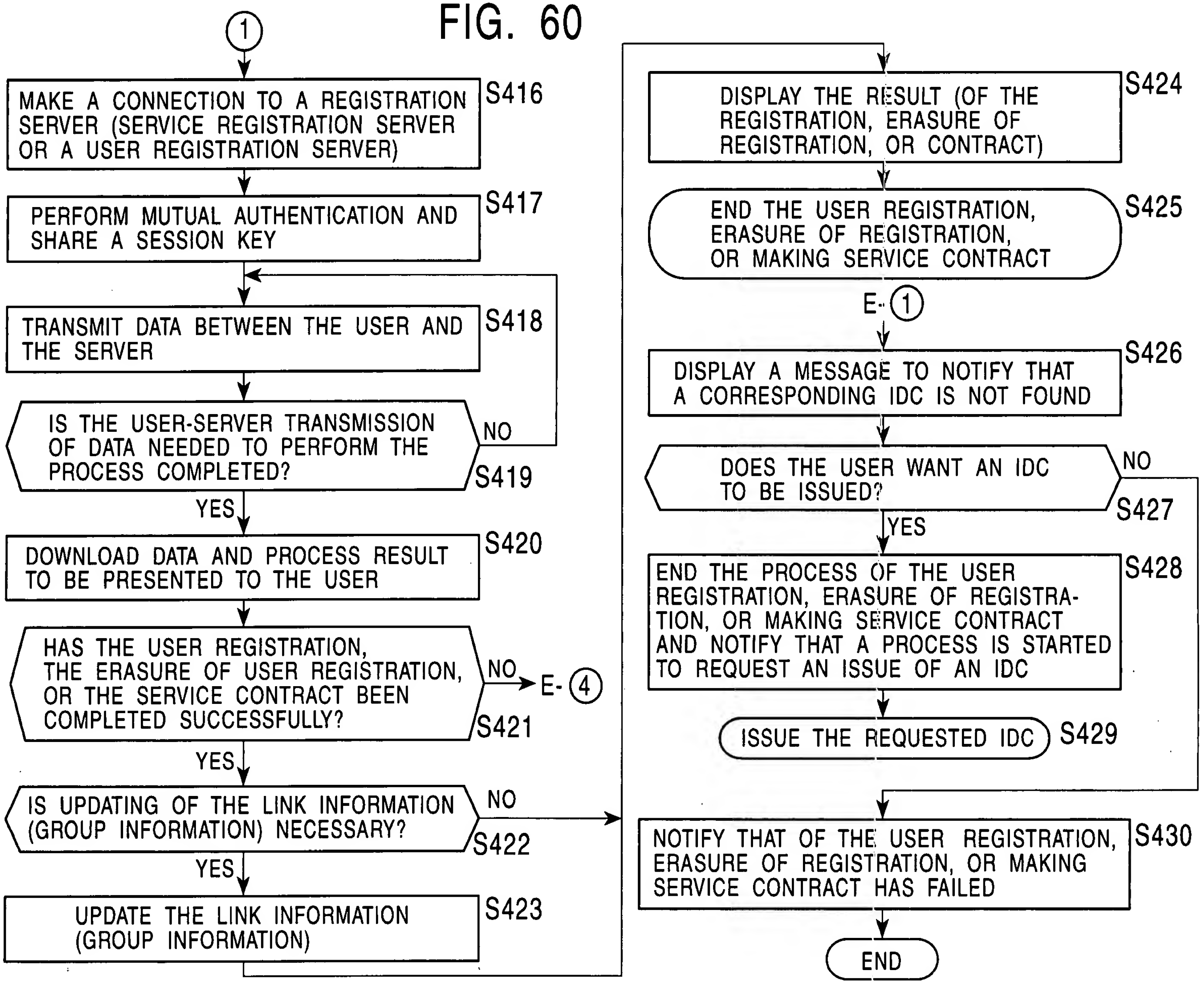

1
MAKE A CONNECTION TO A REGISTRATION SERVER (SERVICE REGISTRATION SERVER OR A USER REGISTRATION SERVER)
S416
PERFORM MUTUAL AUTHENTICATION AND SHARE A SESSION KEY
S417
TRANSMIT DATA BETWEEN THE USER AND THE SERVER
S418
IS THE USER-SERVER TRANSMISSION OF DATA NEEDED TO PERFORM THE PROCESS COMPLETED?
NO
S419
YES
DOWNLOAD DATA AND PROCESS RESULT TO BE PRESENTED TO THE USER
S420
HAS THE USER REGISTRATION, THE ERASURE OF USER REGISTRATION, OR THE SERVICE CONTRACT BEEN COMPLETED SUCCESSFULLY?
NO
E- 4
S421
YES
IS UPDATING OF THE LINK INFORMATION (GROUP INFORMATION) NECESSARY?
NO
S422
YES
UPDATE THE LINK INFORMATION (GROUP INFORMATION)
S423
DISPLAY THE RESULT (OF THE REGISTRATION, ERASURE OF REGISTRATION, OR CONTRACT)
S424
END THE USER REGISTRATION, ERASURE OF REGISTRATION, OR MAKING SERVICE CONTRACT
S425
E- 1
DISPLAY A MESSAGE TO NOTIFY THAT A CORRESPONDING IDC IS NOT FOUND
S426
DOES THE USER WANT AN IDC TO BE ISSUED?
NO
S427
YES
END THE PROCESS OF THE USER REGISTRATION, ERASURE OF REGISTRATION, OR MAKING SERVICE CONTRACT AND NOTIFY THAT A PROCESS IS STARTED TO REQUEST AN ISSUE OF AN IDC
S428
ISSUE THE REQUESTED IDC
S429
NOTIFY THAT OF THE USER REGISTRATION, ERASURE OF REGISTRATION, OR MAKING SERVICE CONTRACT HAS FAILED
S430
END

FIG. 61

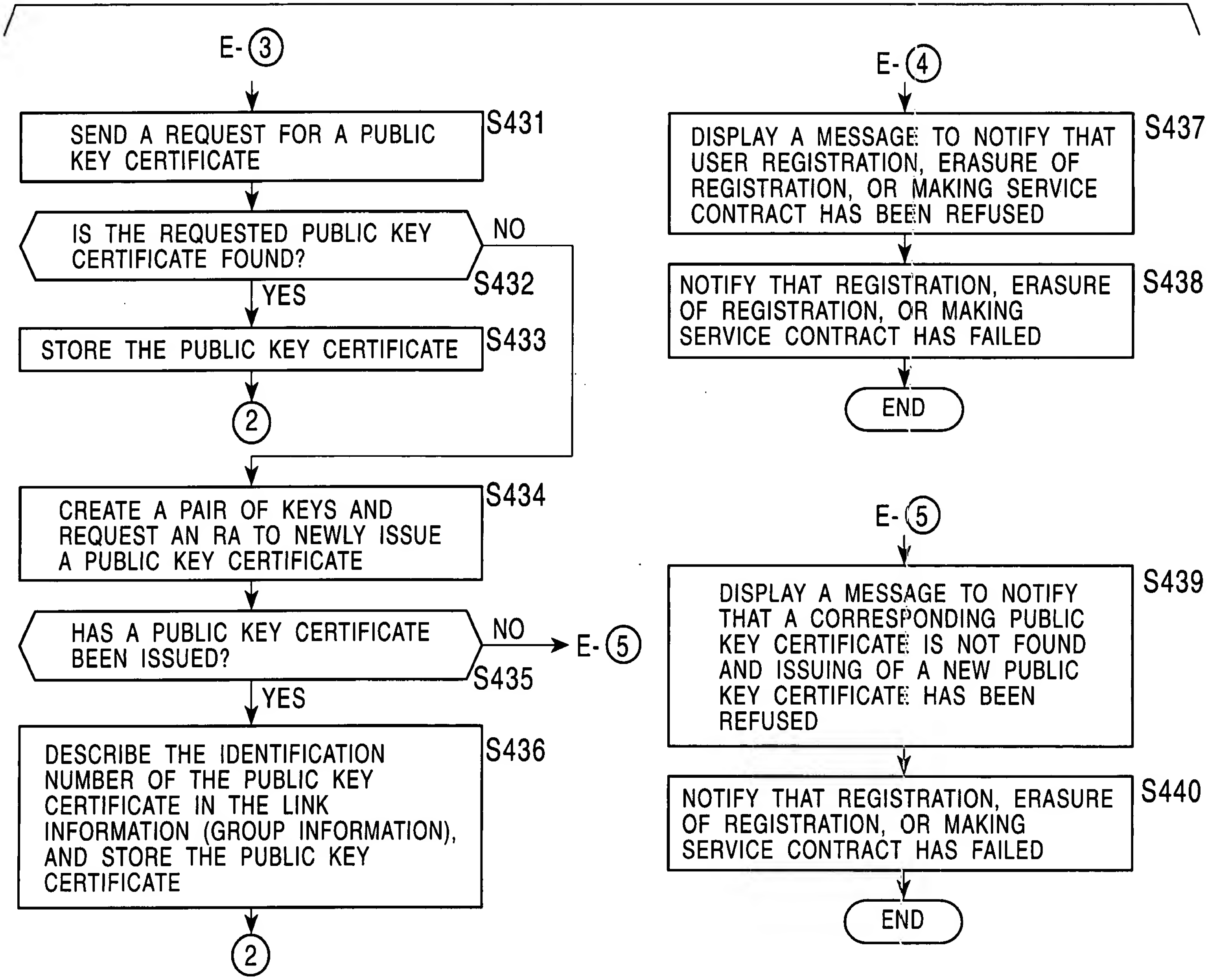

E-3
SEND A REQUEST FOR A PUBLIC KEY CERTIFICATE
S431
IS THE REQUESTED PUBLIC KEY CERTIFICATE FOUND?
S432
NO
YES
STORE THE PUBLIC KEY CERTIFICATE
S433
2
CREATE A PAIR OF KEYS AND REQUEST AN RA TO NEWLY ISSUE A PUBLIC KEY CERTIFICATE
S434
HAS A PUBLIC KEY CERTIFICATE BEEN ISSUED?
S435
NO
E-5
YES
DESCRIBE THE IDENTIFICATION NUMBER OF THE PUBLIC KEY CERTIFICATE IN THE LINK INFORMATION (GROUP INFORMATION), AND STORE THE PUBLIC KEY CERTIFICATE
S436
2
E-4
DISPLAY A MESSAGE TO NOTIFY THAT USER REGISTRATION, ERASURE OF REGISTRATION, OR MAKING SERVICE CONTRACT HAS BEEN REFUSED
S437
NOTIFY THAT REGISTRATION, ERASURE OF REGISTRATION, OR MAKING SERVICE CONTRACT HAS FAILED
S438
END
E-5
DISPLAY A MESSAGE TO NOTIFY THAT A CORRESPONDING PUBLIC KEY CERTIFICATE IS NOT FOUND AND ISSUING OF A NEW PUBLIC KEY CERTIFICATE HAS BEEN REFUSED
S439
NOTIFY THAT REGISTRATION, ERASURE OF REGISTRATION, OR MAKING SERVICE CONTRACT HAS FAILED
S440
END

FIG. 62

PRECONDITIONS:

- AN IDC OF INTEREST HAS NOT BEEN REGISTERED IN THE USER DEVICE
- THE USER DEVICE HAS NEITHER A PKC NOR A PAIR OF KEYS BUT THE USER DEVICE CAN CREATE THEM
- AN OFF-LINE PROCEDURE NEEDED TO ISSUE AN IDC HAS BEEN PERFORMED, AND INFORMATION (PIN, TEMPLATE, OR SIGNATURE ENCRYPTED USING A PRIVATE KEY) USED TO CHECK WHETHER A TEMPLATE SUPPLIER IS IDENTICAL TO AN APPLICANT HAS BEEN DETERMINED

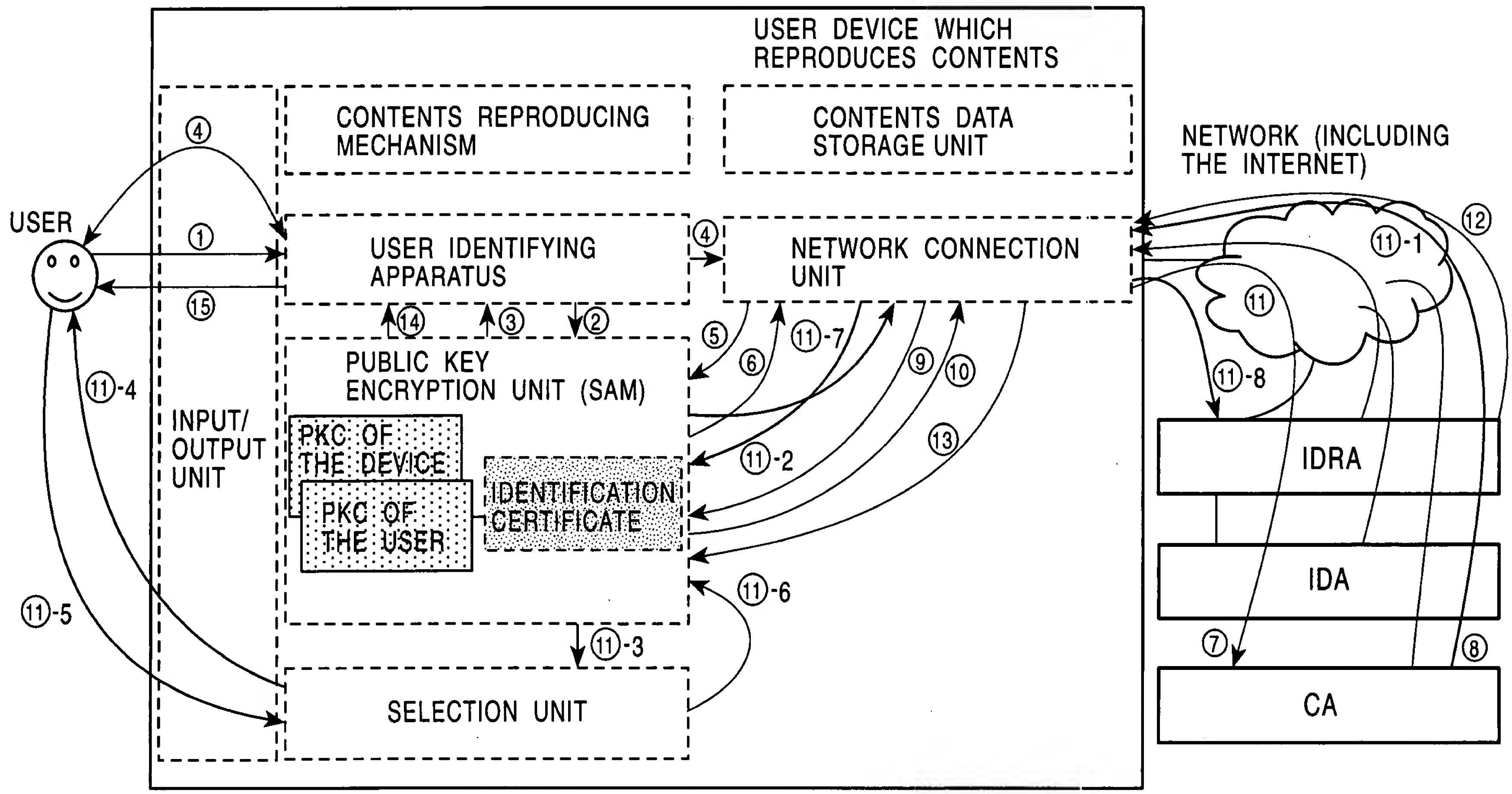

USER
USER DEVICE WHICH REPRODUCES CONTENTS
CONTENTS REPRODUCING MECHANISM
CONTENTS DATA STORAGE UNIT
NETWORK (INCLUDING THE INTERNET)
USER IDENTIFYING APPARATUS
NETWORK CONNECTION UNIT
PUBLIC KEY ENCRYPTION UNIT (SAM)
PKC OF THE DEVICE
PKC OF THE USER
IDENTIFICATION CERTIFICATE
INPUT/ OUTPUT UNIT
SELECTION UNIT
IDRA
IDA
CA
①
②
③
④
④
⑤
⑥
⑦
⑧
⑨
⑩
⑪
⑪-1
⑪-2
⑪-3
⑪-4
⑪-5
⑪-6
⑪-7
⑪-8
⑫
⑬
⑭
⑮

FIG. 63

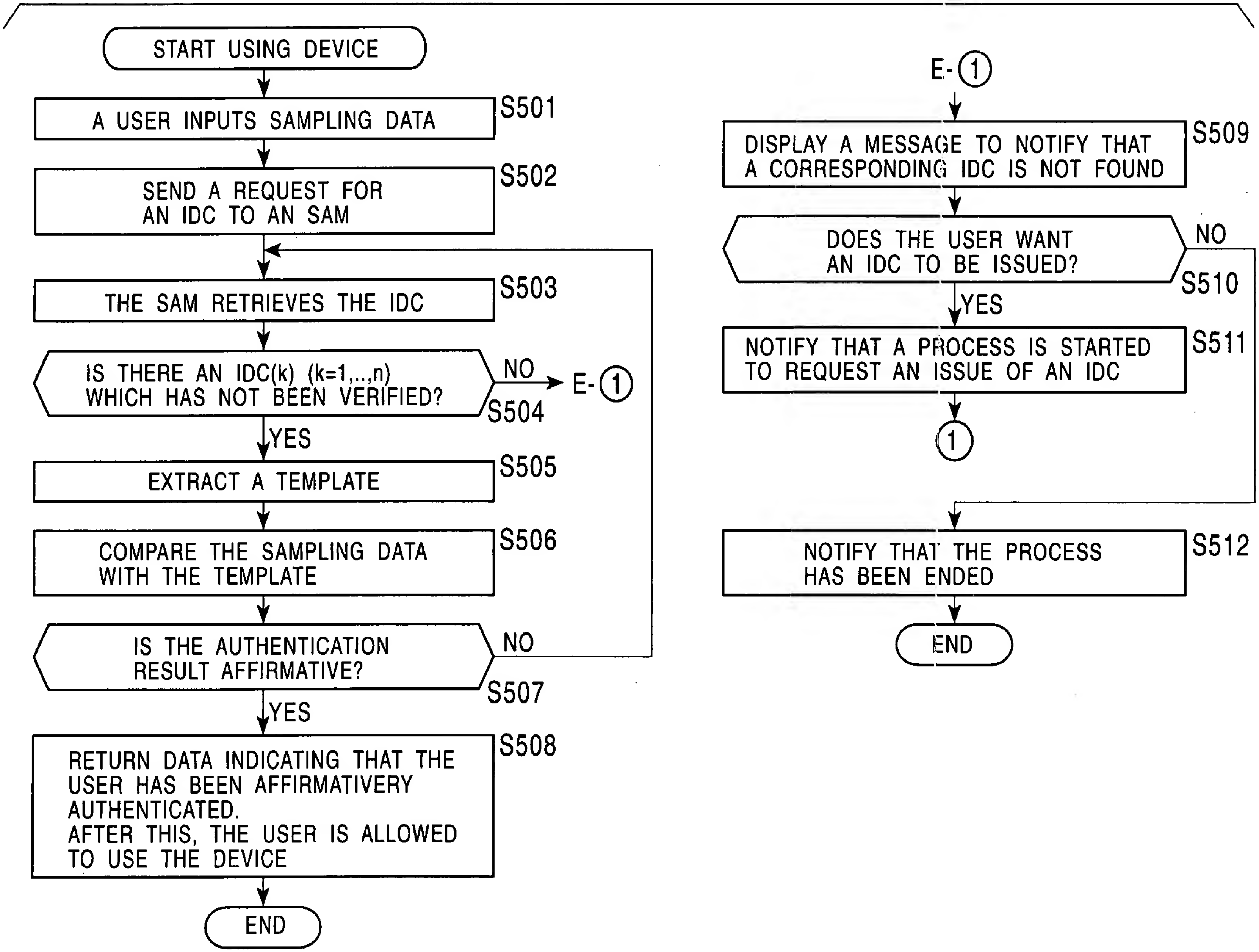

START USING DEVICE
A USER INPUTS SAMPLING DATA
S501
SEND A REQUEST FOR AN IDC TO AN SAM
S502
THE SAM RETRIEVES THE IDC
S503
IS THERE AN IDC(k) (k=1,..,n) WHICH HAS NOT BEEN VERIFIED?
S504
NO
E-1
YES
EXTRACT A TEMPLATE
S505
COMPARE THE SAMPLING DATA WITH THE TEMPLATE
S506
IS THE AUTHENTICATION RESULT AFFIRMATIVE?
S507
NO
YES
RETURN DATA INDICATING THAT THE USER HAS BEEN AFFIRMATIVERY AUTHENTICATED.
AFTER THIS, THE USER IS ALLOWED TO USE THE DEVICE
S508
END
E-1
DISPLAY A MESSAGE TO NOTIFY THAT A CORRESPONDING IDC IS NOT FOUND
S509
DOES THE USER WANT AN IDC TO BE ISSUED?
S510
NO
YES
NOTIFY THAT A PROCESS IS STARTED TO REQUEST AN ISSUE OF AN IDC
S511
1
NOTIFY THAT THE PROCESS HAS BEEN ENDED
S512
END

FIG. 64

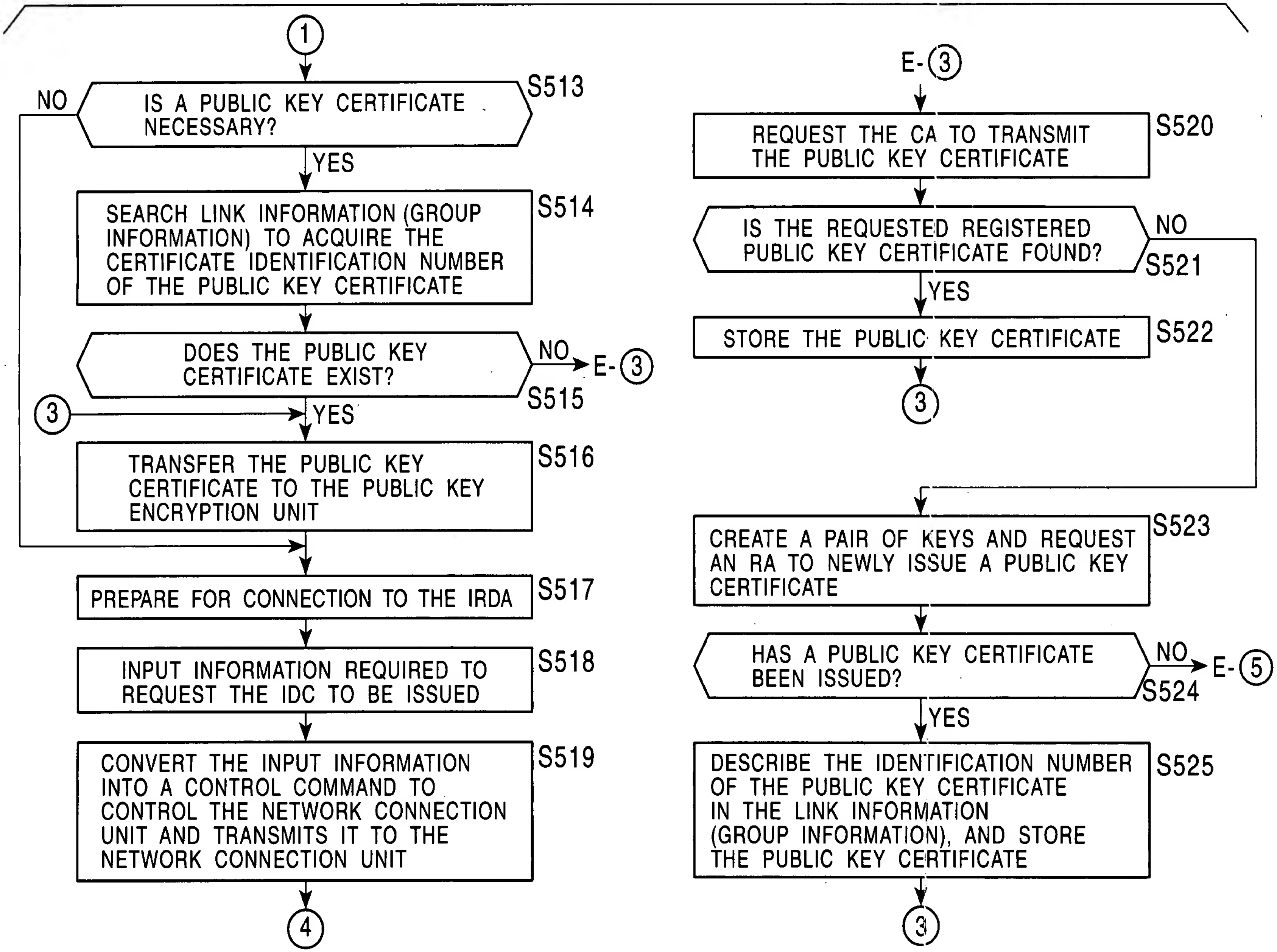

1
IS A PUBLIC KEY CERTIFICATE NECESSARY?
S513
NO
YES
SEARCH LINK INFORMATION (GROUP INFORMATION) TO ACQUIRE THE CERTIFICATE IDENTIFICATION NUMBER OF THE PUBLIC KEY CERTIFICATE
S514
DOES THE PUBLIC KEY CERTIFICATE EXIST?
NO
E-3
S515
3
YES
TRANSFER THE PUBLIC KEY CERTIFICATE TO THE PUBLIC KEY ENCRYPTION UNIT
S516
PREPARE FOR CONNECTION TO THE IRDA
S517
INPUT INFORMATION REQUIRED TO REQUEST THE IDC TO BE ISSUED
S518
CONVERT THE INPUT INFORMATION INTO A CONTROL COMMAND TO CONTROL THE NETWORK CONNECTION UNIT AND TRANSMITS IT TO THE NETWORK CONNECTION UNIT
S519
4
E-3
REQUEST THE CA TO TRANSMIT THE PUBLIC KEY CERTIFICATE
S520
IS THE REQUESTED REGISTERED PUBLIC KEY CERTIFICATE FOUND?
NO
S521
YES
STORE THE PUBLIC KEY CERTIFICATE
S522
3
CREATE A PAIR OF KEYS AND REQUEST AN RA TO NEWLY ISSUE A PUBLIC KEY CERTIFICATE
S523
HAS A PUBLIC KEY CERTIFICATE BEEN ISSUED?
NO
E-5
S524
YES
DESCRIBE THE IDENTIFICATION NUMBER OF THE PUBLIC KEY CERTIFICATE IN THE LINK INFORMATION (GROUP INFORMATION), AND STORE THE PUBLIC KEY CERTIFICATE
S525
3

FIG. 65

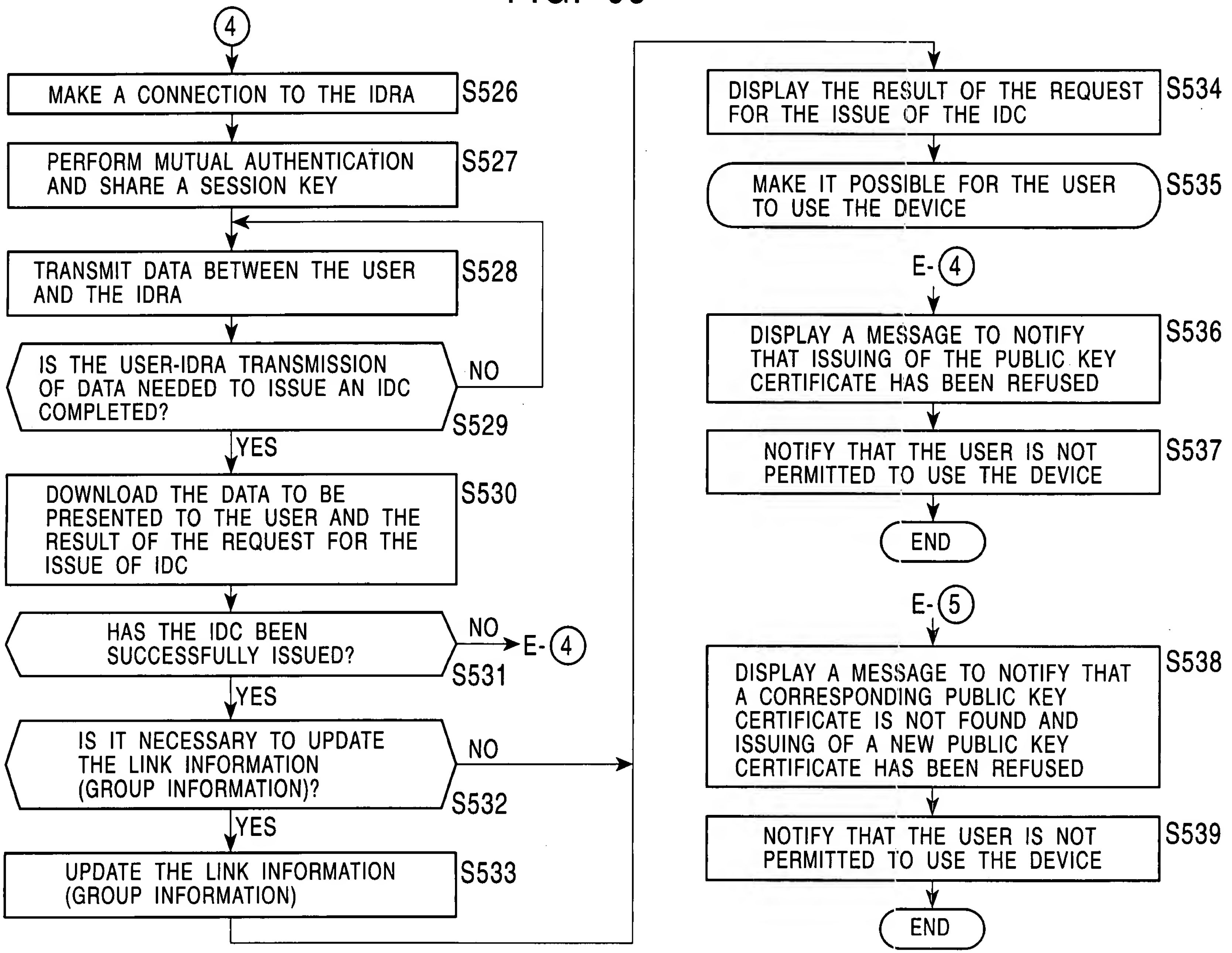

4
MAKE A CONNECTION TO THE IDRA
S526
PERFORM MUTUAL AUTHENTICATION AND SHARE A SESSION KEY
S527
TRANSMIT DATA BETWEEN THE USER AND THE IDRA
S528
IS THE USER-IDRA TRANSMISSION OF DATA NEEDED TO ISSUE AN IDC COMPLETED?
NO
S529
YES
DOWNLOAD THE DATA TO BE PRESENTED TO THE USER AND THE RESULT OF THE REQUEST FOR THE ISSUE OF IDC
S530
HAS THE IDC BEEN SUCCESSFULLY ISSUED?
NO
E-4
S531
YES
IS IT NECESSARY TO UPDATE THE LINK INFORMATION (GROUP INFORMATION)?
NO
S532
YES
UPDATE THE LINK INFORMATION (GROUP INFORMATION)
S533
DISPLAY THE RESULT OF THE REQUEST FOR THE ISSUE OF THE IDC
S534
MAKE IT POSSIBLE FOR THE USER TO USE THE DEVICE
S535
E-4
DISPLAY A MESSAGE TO NOTIFY THAT ISSUING OF THE PUBLIC KEY CERTIFICATE HAS BEEN REFUSED
S536
NOTIFY THAT THE USER IS NOT PERMITTED TO USE THE DEVICE
S537
END
E-5
DISPLAY A MESSAGE TO NOTIFY THAT A CORRESPONDING PUBLIC KEY CERTIFICATE IS NOT FOUND AND ISSUING OF A NEW PUBLIC KEY CERTIFICATE HAS BEEN REFUSED
S538
NOTIFY THAT THE USER IS NOT PERMITTED TO USE THE DEVICE
S539
END

FIG. 66

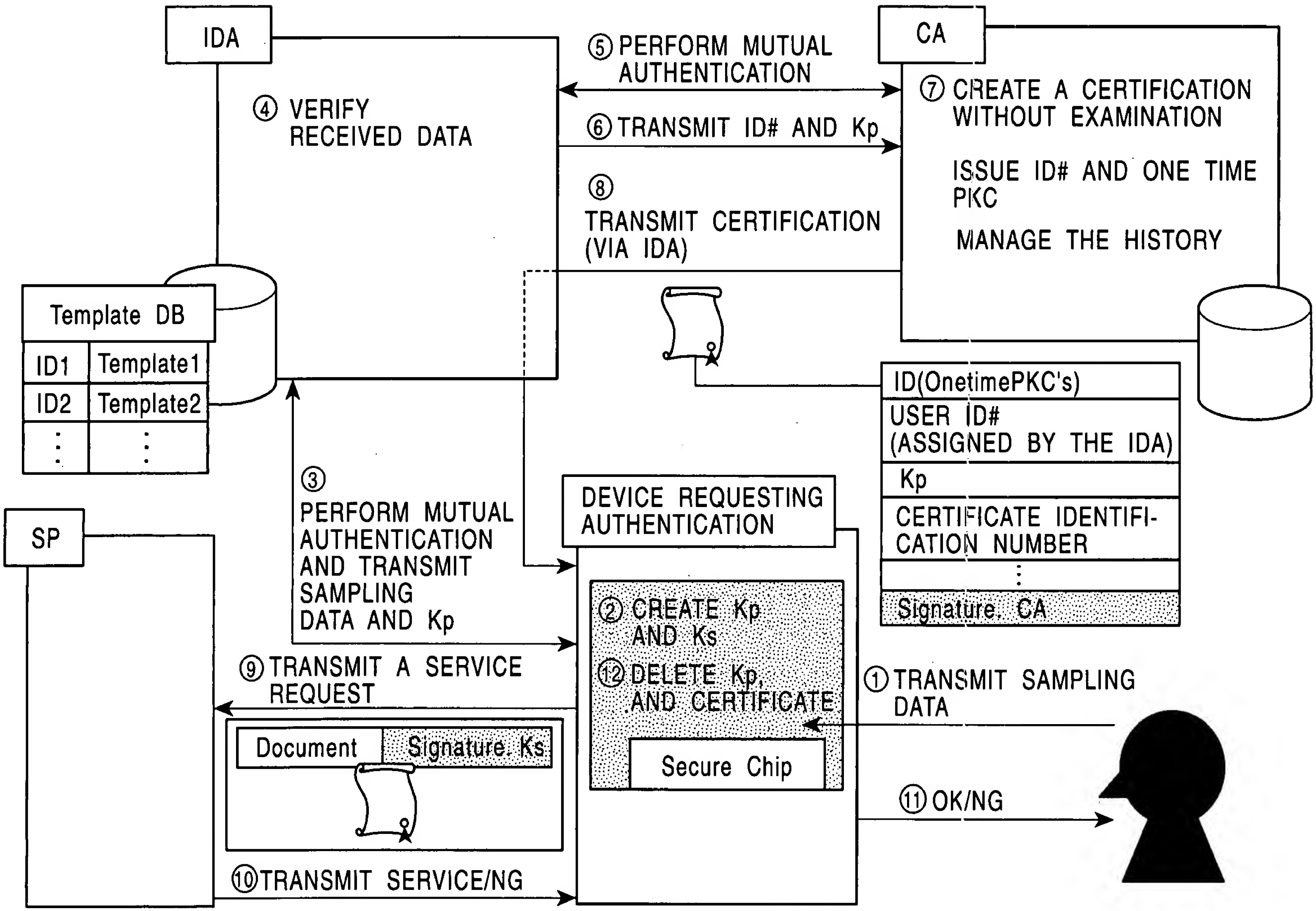

IDA
④ VERIFY RECEIVED DATA
Template DB
ID1 Template1
ID2 Template2
⑤ PERFORM MUTUAL AUTHENTICATION
⑥ TRANSMIT ID# AND Kp
⑧ TRANSMIT CERTIFICATION (VIA IDA)
CA
⑦ CREATE A CERTIFICATION WITHOUT EXAMINATION
ISSUE ID# AND ONE TIME PKC
MANAGE THE HISTORY
ID(OnetimePKC's)
USER ID# (ASSIGNED BY THE IDA)
Kp
CERTIFICATE IDENTIFICATION NUMBER
Signature. CA
③ PERFORM MUTUAL AUTHENTICATION AND TRANSMIT SAMPLING DATA AND Kp
DEVICE REQUESTING AUTHENTICATION
② CREATE Kp AND Ks
⑫ DELETE Kp, AND CERTIFICATE
Secure Chip
① TRANSMIT SAMPLING DATA
⑪ OK/NG
SP
⑨ TRANSMIT A SERVICE REQUEST
Document
Signature. Ks
⑩ TRANSMIT SERVICE/NG

FIG. 67

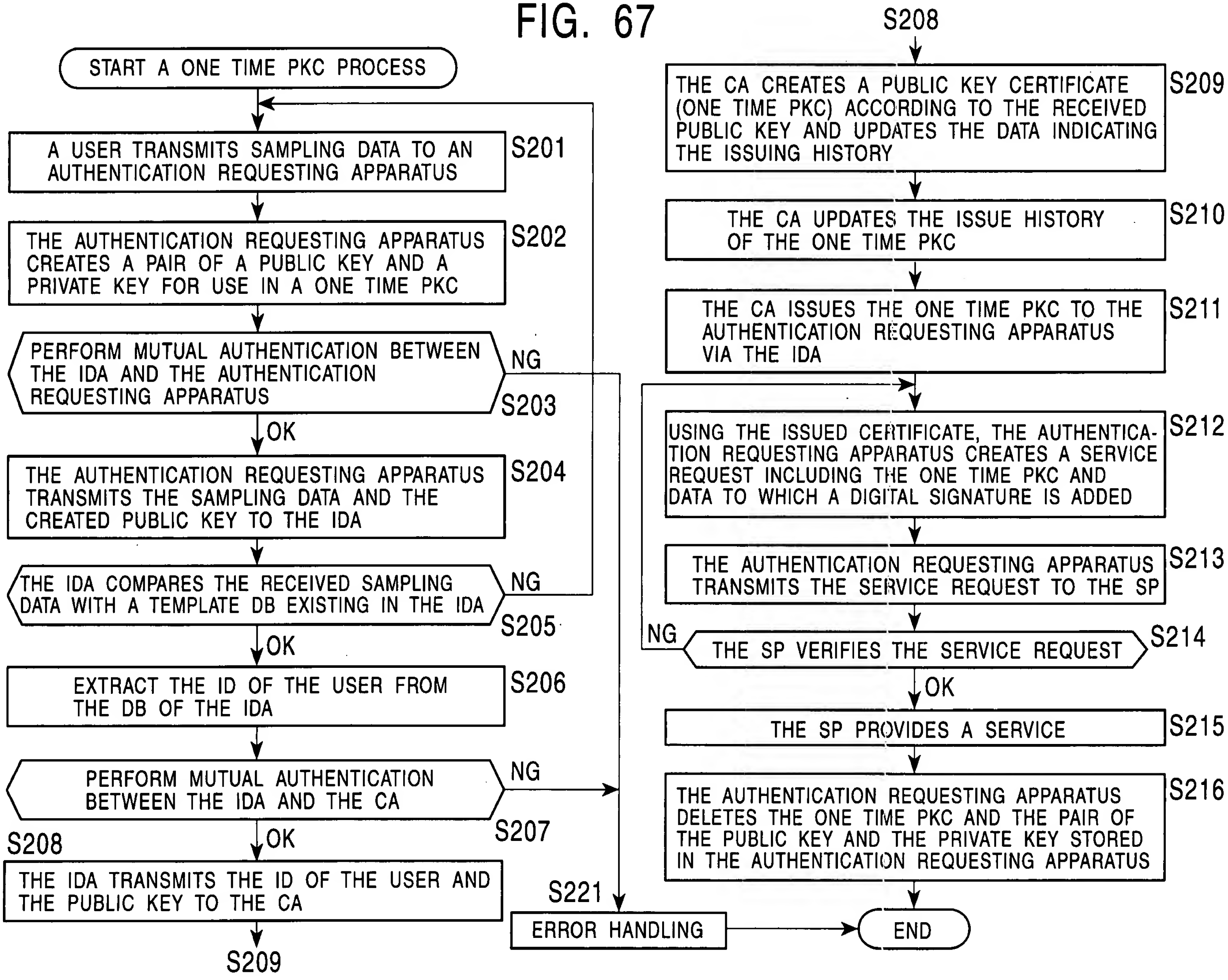

START A ONE TIME PKC PROCESS
A USER TRANSMITS SAMPLING DATA TO AN AUTHENTICATION REQUESTING APPARATUS
S201
THE AUTHENTICATION REQUESTING APPARATUS CREATES A PAIR OF A PUBLIC KEY AND A PRIVATE KEY FOR USE IN A ONE TIME PKC
S202
PERFORM MUTUAL AUTHENTICATION BETWEEN THE IDA AND THE AUTHENTICATION REQUESTING APPARATUS
NG
S203
OK
THE AUTHENTICATION REQUESTING APPARATUS TRANSMITS THE SAMPLING DATA AND THE CREATED PUBLIC KEY TO THE IDA
S204
THE IDA COMPARES THE RECEIVED SAMPLING DATA WITH A TEMPLATE DB EXISTING IN THE IDA
NG
S205
OK
EXTRACT THE ID OF THE USER FROM THE DB OF THE IDA
S206
PERFORM MUTUAL AUTHENTICATION BETWEEN THE IDA AND THE CA
NG
S207
OK
S208
THE IDA TRANSMITS THE ID OF THE USER AND THE PUBLIC KEY TO THE CA
S209
S221
ERROR HANDLING
S208
THE CA CREATES A PUBLIC KEY CERTIFICATE (ONE TIME PKC) ACCORDING TO THE RECEIVED PUBLIC KEY AND UPDATES THE DATA INDICATING THE ISSUING HISTORY
S209
THE CA UPDATES THE ISSUE HISTORY OF THE ONE TIME PKC
S210
THE CA ISSUES THE ONE TIME PKC TO THE AUTHENTICATION REQUESTING APPARATUS VIA THE IDA
S211
USING THE ISSUED CERTIFICATE, THE AUTHENTICATION REQUESTING APPARATUS CREATES A SERVICE REQUEST INCLUDING THE ONE TIME PKC AND DATA TO WHICH A DIGITAL SIGNATURE IS ADDED
S212
THE AUTHENTICATION REQUESTING APPARATUS TRANSMITS THE SERVICE REQUEST TO THE SP
S213
NG
THE SP VERIFIES THE SERVICE REQUEST
S214
OK
THE SP PROVIDES A SERVICE
S215
THE AUTHENTICATION REQUESTING APPARATUS DELETES THE ONE TIME PKC AND THE PAIR OF THE PUBLIC KEY AND THE PRIVATE KEY STORED IN THE AUTHENTICATION REQUESTING APPARATUS
S216
END

FIG. 68

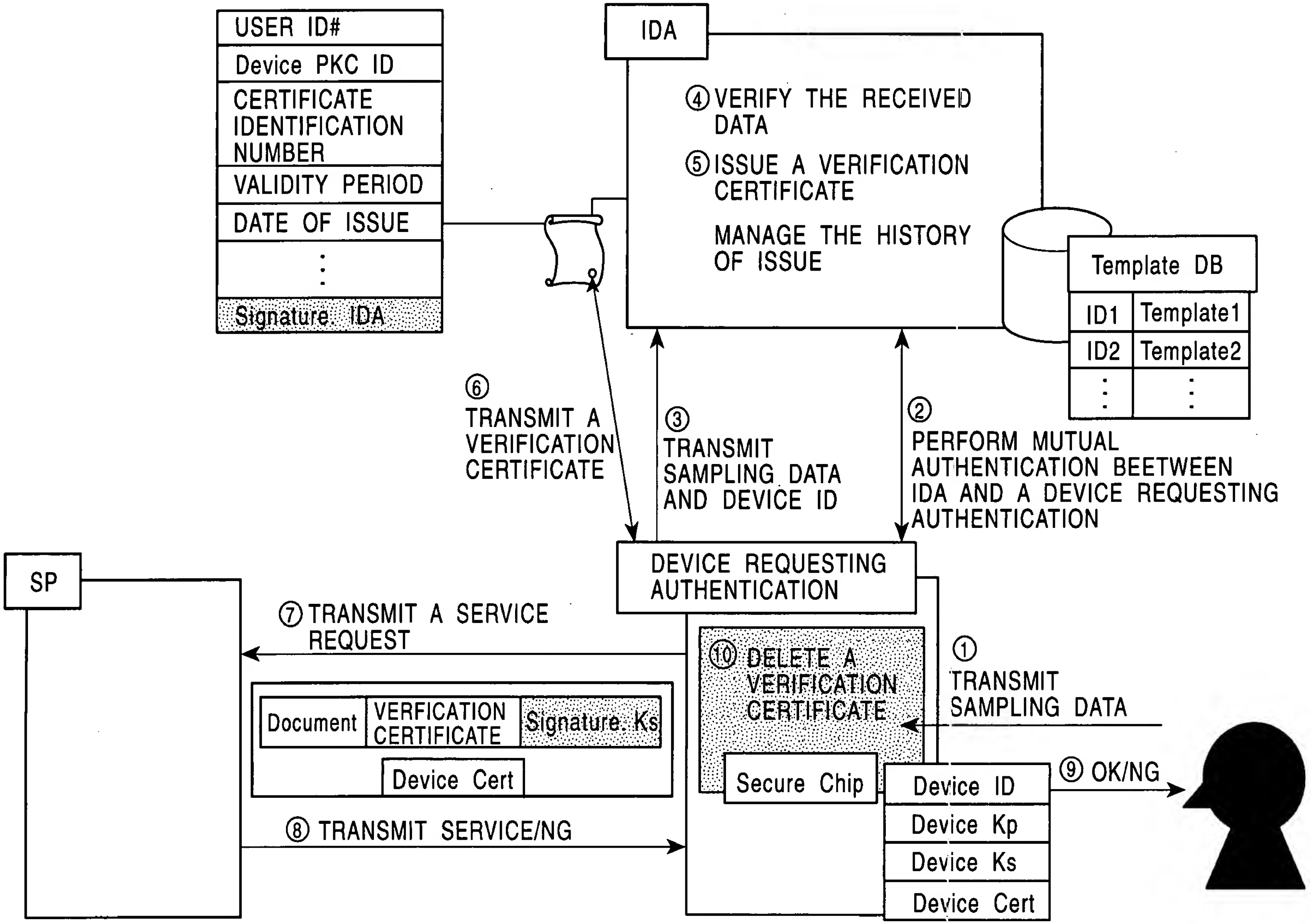

USER ID#
Device PKC ID
CERTIFICATE IDENTIFICATION NUMBER
VALIDITY PERIOD
DATE OF ISSUE
⋮
Signature. IDA
IDA
④ VERIFY THE RECEIVED DATA
⑤ ISSUE A VERIFICATION CERTIFICATE
MANAGE THE HISTORY OF ISSUE
Template DB
ID1
Template1
ID2
Template2
⋮
⋮
⑥ TRANSMIT A VERIFICATION CERTIFICATE
③ TRANSMIT SAMPLING DATA AND DEVICE ID
② PERFORM MUTUAL AUTHENTICATION BEETWEEN IDA AND A DEVICE REQUESTING AUTHENTICATION
SP
DEVICE REQUESTING AUTHENTICATION
⑦ TRANSMIT A SERVICE REQUEST
⑩ DELETE A VERIFICATION CERTIFICATE
① TRANSMIT SAMPLING DATA
Document
VERFICATION CERTIFICATE
Signature. Ks
Device Cert
Secure Chip
Device ID
Device Kp
Device Ks
Device Cert
⑨ OK/NG
⑧ TRANSMIT SERVICE/NG

FIG. 69

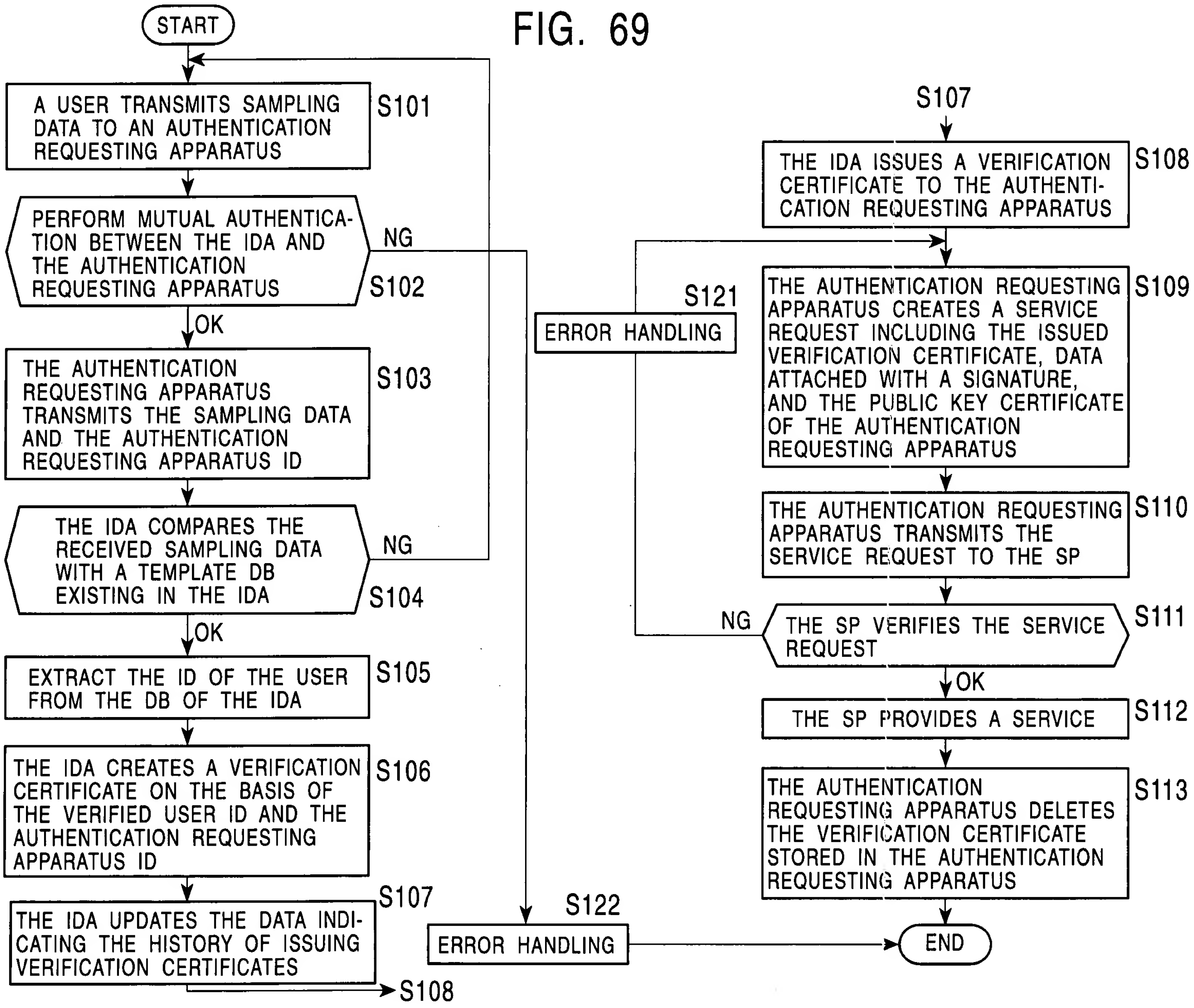

START
A USER TRANSMITS SAMPLING DATA TO AN AUTHENTICATION REQUESTING APPARATUS
S101
PERFORM MUTUAL AUTHENTICATION BETWEEN THE IDA AND THE AUTHENTICATION REQUESTING APPARATUS
S102
NG
OK
THE AUTHENTICATION REQUESTING APPARATUS TRANSMITS THE SAMPLING DATA AND THE AUTHENTICATION REQUESTING APPARATUS ID
S103
THE IDA COMPARES THE RECEIVED SAMPLING DATA WITH A TEMPLATE DB EXISTING IN THE IDA
S104
NG
OK
EXTRACT THE ID OF THE USER FROM THE DB OF THE IDA
S105
THE IDA CREATES A VERIFICATION CERTIFICATE ON THE BASIS OF THE VERIFIED USER ID AND THE AUTHENTICATION REQUESTING APPARATUS ID
S106
THE IDA UPDATES THE DATA INDICATING THE HISTORY OF ISSUING VERIFICATION CERTIFICATES
S107
S108
ERROR HANDLING
S122
S107
THE IDA ISSUES A VERIFICATION CERTIFICATE TO THE AUTHENTICATION REQUESTING APPARATUS
S108
ERROR HANDLING
S121
THE AUTHENTICATION REQUESTING APPARATUS CREATES A SERVICE REQUEST INCLUDING THE ISSUED VERIFICATION CERTIFICATE, DATA ATTACHED WITH A SIGNATURE, AND THE PUBLIC KEY CERTIFICATE OF THE AUTHENTICATION REQUESTING APPARATUS
S109
THE AUTHENTICATION REQUESTING APPARATUS TRANSMITS THE SERVICE REQUEST TO THE SP
S110
NG
THE SP VERIFIES THE SERVICE REQUEST
S111
OK
THE SP PROVIDES A SERVICE
S112
THE AUTHENTICATION REQUESTING APPARATUS DELETES THE VERIFICATION CERTIFICATE STORED IN THE AUTHENTICATION REQUESTING APPARATUS
S113
END

FIG. 70

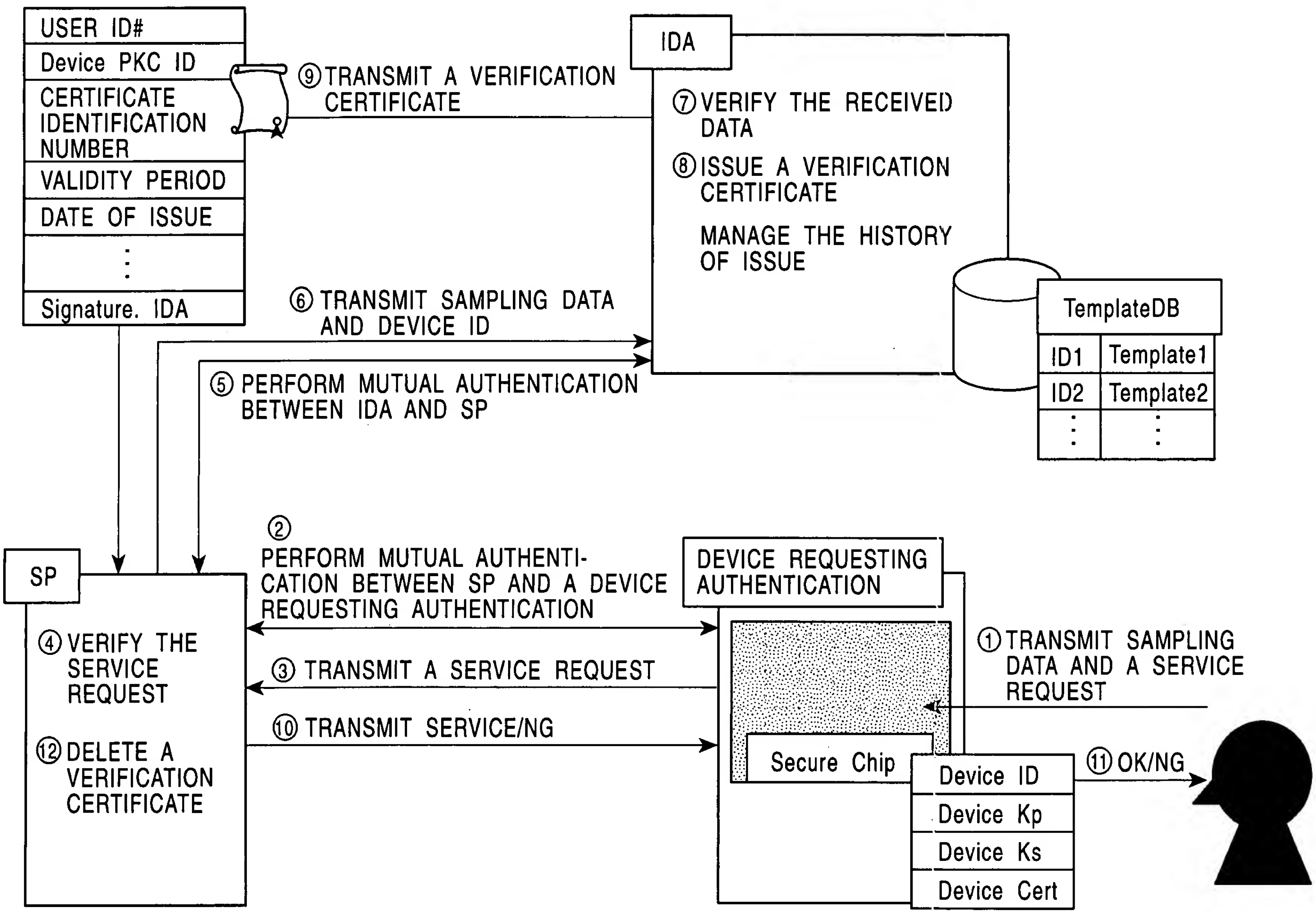

USER ID#
Device PKC ID
CERTIFICATE IDENTIFICATION NUMBER
VALIDITY PERIOD
DATE OF ISSUE
⋮
Signature. IDA
⑨TRANSMIT A VERIFICATION CERTIFICATE
IDA
⑦VERIFY THE RECEIVED DATA
⑧ISSUE A VERIFICATION CERTIFICATE
MANAGE THE HISTORY OF ISSUE
TemplateDB
ID1
Template1
ID2
Template2
⋮
⋮
⑥TRANSMIT SAMPLING DATA AND DEVICE ID
⑤PERFORM MUTUAL AUTHENTICATION BETWEEN IDA AND SP
② PERFORM MUTUAL AUTHENTI-CATION BETWEEN SP AND A DEVICE REQUESTING AUTHENTICATION
DEVICE REQUESTING AUTHENTICATION
SP
④VERIFY THE SERVICE REQUEST
⑫DELETE A VERIFICATION CERTIFICATE
③TRANSMIT A SERVICE REQUEST
⑩TRANSMIT SERVICE/NG
①TRANSMIT SAMPLING DATA AND A SERVICE REQUEST
Secure Chip
Device ID
Device Kp
Device Ks
Device Cert
⑪OK/NG

FIG. 71

	Item	Description
Indis-pensable Items	Version	Version
	Serial Number	Identification Number
	signature algorithm Identifier algorithm parameters	Signature algorithm Algorithm Parameters
	Issuer	Identification authority name (in the form of a distinguished name)
	Validity notBefore notAfter	Validty period • Start date • Expiration date
	Subject	Subject Name (in a DN form)
	subject IDA Info subject IDA serial Number subject IDA Unique ID	Information about the identification cartificate of the subject • Certificate number of the identification certificate of the subject • Subject unique ID of the identification cerificate of the subject
	subject PKC info subject PKC serial Number subject PKC Unique ID	Information about the public key certificate of the subject • Certificate Number of the public key certificate of the subject • Subject unique ID of the public key certificate of the subject
Indispen-sable	IDA Signature	Signature of IDA

FIG. 72

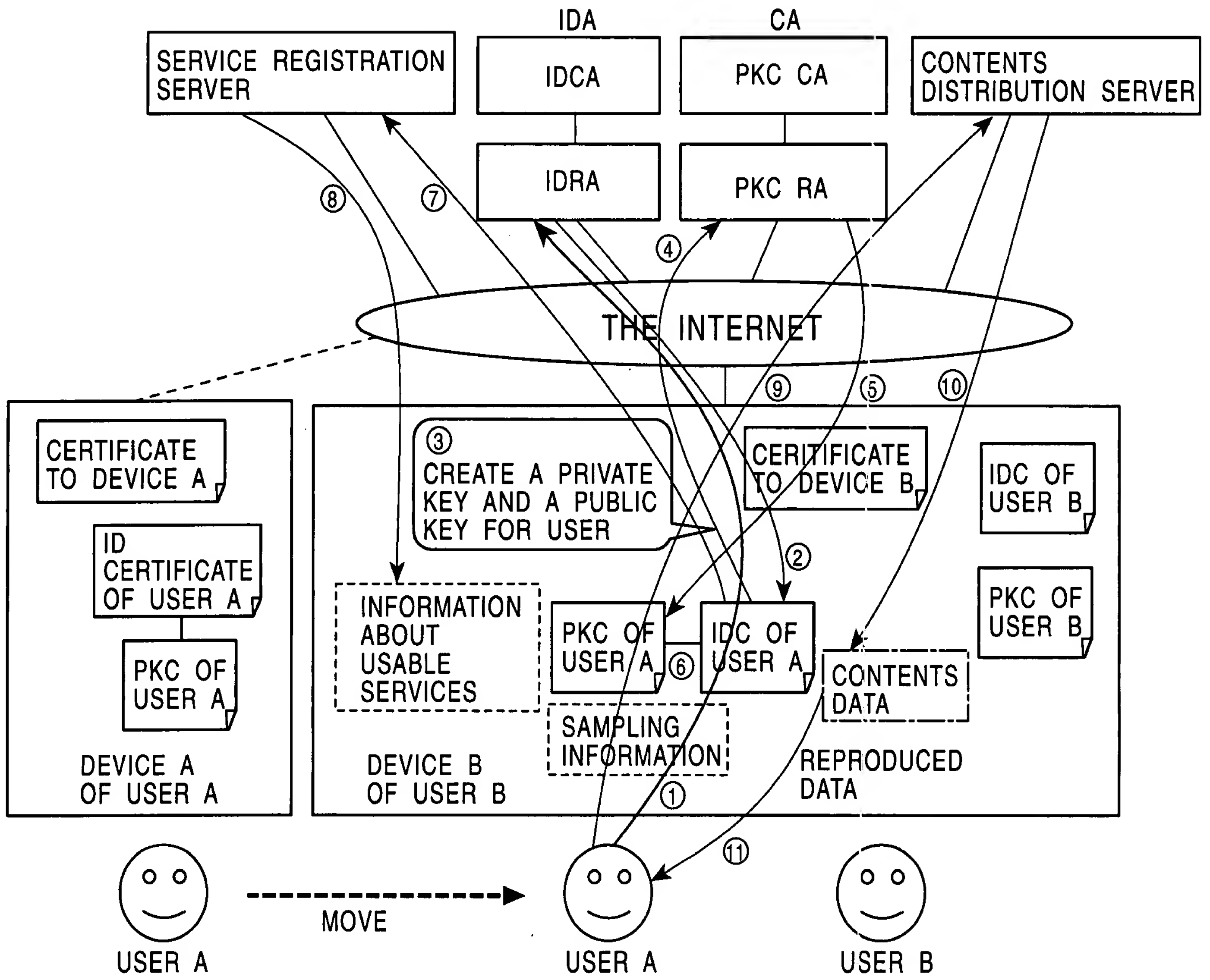

SERVICE REGISTRATION SERVER
IDA
IDCA
IDRA
CA
PKC CA
PKC RA
CONTENTS DISTRIBUTION SERVER
THE INTERNET
⑧
⑦
④
⑨
⑤
⑩
CERTIFICATE TO DEVICE A
ID CERTIFICATE OF USER A
PKC OF USER A
DEVICE A OF USER A
③ CREATE A PRIVATE KEY AND A PUBLIC KEY FOR USER
CERITIFICATE TO DEVICE B
IDC OF USER B
PKC OF USER B
INFORMATION ABOUT USABLE SERVICES
PKC OF USER A
⑥
IDC OF USER A
②
CONTENTS DATA
SAMPLING INFORMATION
①
REPRODUCED DATA
DEVICE B OF USER B
⑪
USER A
MOVE
USER A
USER B

FIG. 73

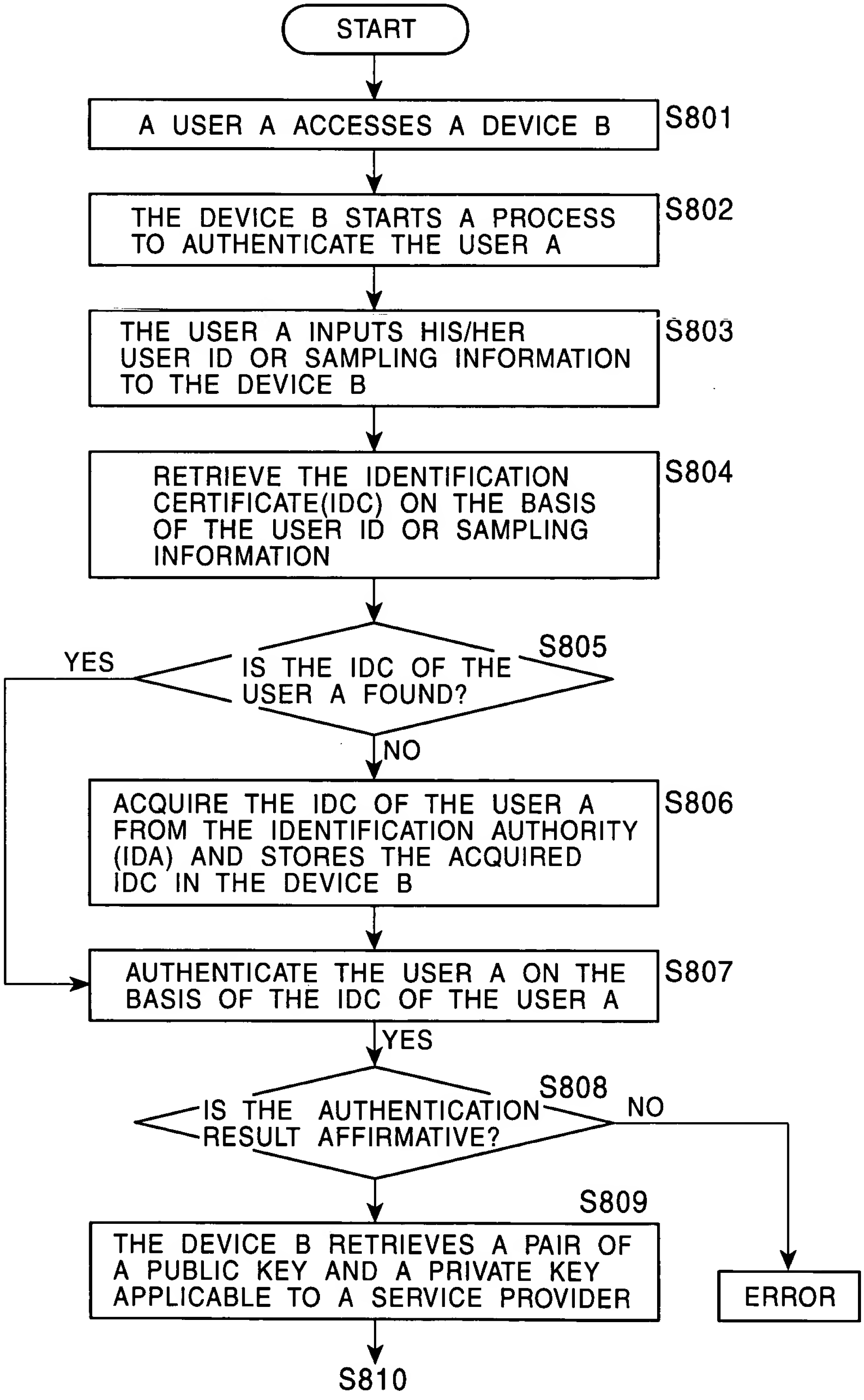

START
A USER A ACCESSES A DEVICE B
S801
THE DEVICE B STARTS A PROCESS TO AUTHENTICATE THE USER A
S802
THE USER A INPUTS HIS/HER USER ID OR SAMPLING INFORMATION TO THE DEVICE B
S803
RETRIEVE THE IDENTIFICATION CERTIFICATE(IDC) ON THE BASIS OF THE USER ID OR SAMPLING INFORMATION
S804
IS THE IDC OF THE USER A FOUND?
S805
YES
NO
ACQUIRE THE IDC OF THE USER A FROM THE IDENTIFICATION AUTHORITY (IDA) AND STORES THE ACQUIRED IDC IN THE DEVICE B
S806
AUTHENTICATE THE USER A ON THE BASIS OF THE IDC OF THE USER A
S807
YES
IS THE AUTHENTICATION RESULT AFFIRMATIVE?
S808
NO
THE DEVICE B RETRIEVES A PAIR OF A PUBLIC KEY AND A PRIVATE KEY APPLICABLE TO A SERVICE PROVIDER
S809
ERROR
S810

FIG. 74

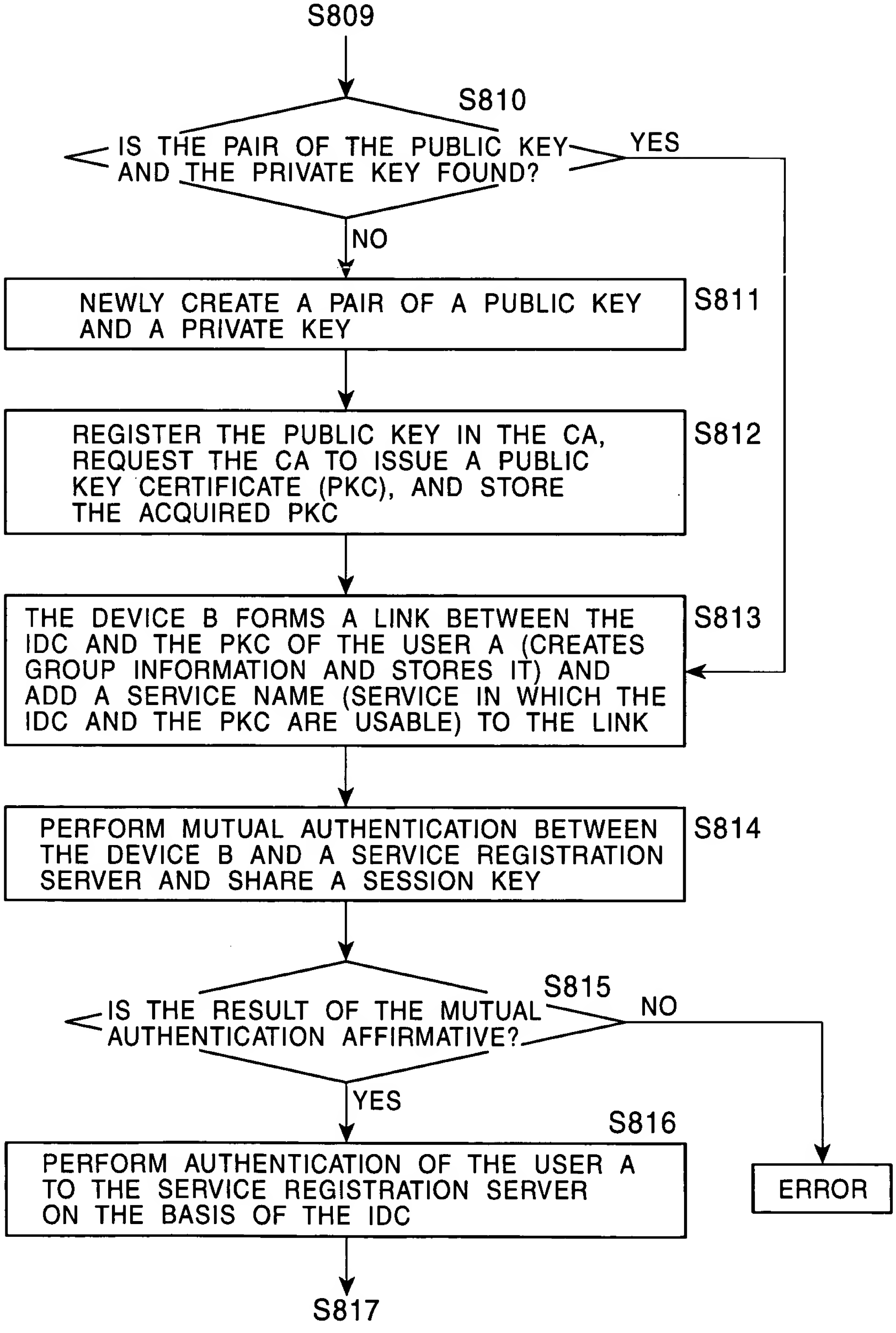

S809
S810
IS THE PAIR OF THE PUBLIC KEY AND THE PRIVATE KEY FOUND?
YES
NO
NEWLY CREATE A PAIR OF A PUBLIC KEY AND A PRIVATE KEY
S811
REGISTER THE PUBLIC KEY IN THE CA, REQUEST THE CA TO ISSUE A PUBLIC KEY CERTIFICATE (PKC), AND STORE THE ACQUIRED PKC
S812
THE DEVICE B FORMS A LINK BETWEEN THE IDC AND THE PKC OF THE USER A (CREATES GROUP INFORMATION AND STORES IT) AND ADD A SERVICE NAME (SERVICE IN WHICH THE IDC AND THE PKC ARE USABLE) TO THE LINK
S813
PERFORM MUTUAL AUTHENTICATION BETWEEN THE DEVICE B AND A SERVICE REGISTRATION SERVER AND SHARE A SESSION KEY
S814
S815
IS THE RESULT OF THE MUTUAL AUTHENTICATION AFFIRMATIVE?
NO
YES
S816
PERFORM AUTHENTICATION OF THE USER A TO THE SERVICE REGISTRATION SERVER ON THE BASIS OF THE IDC
ERROR
S817

FIG. 75

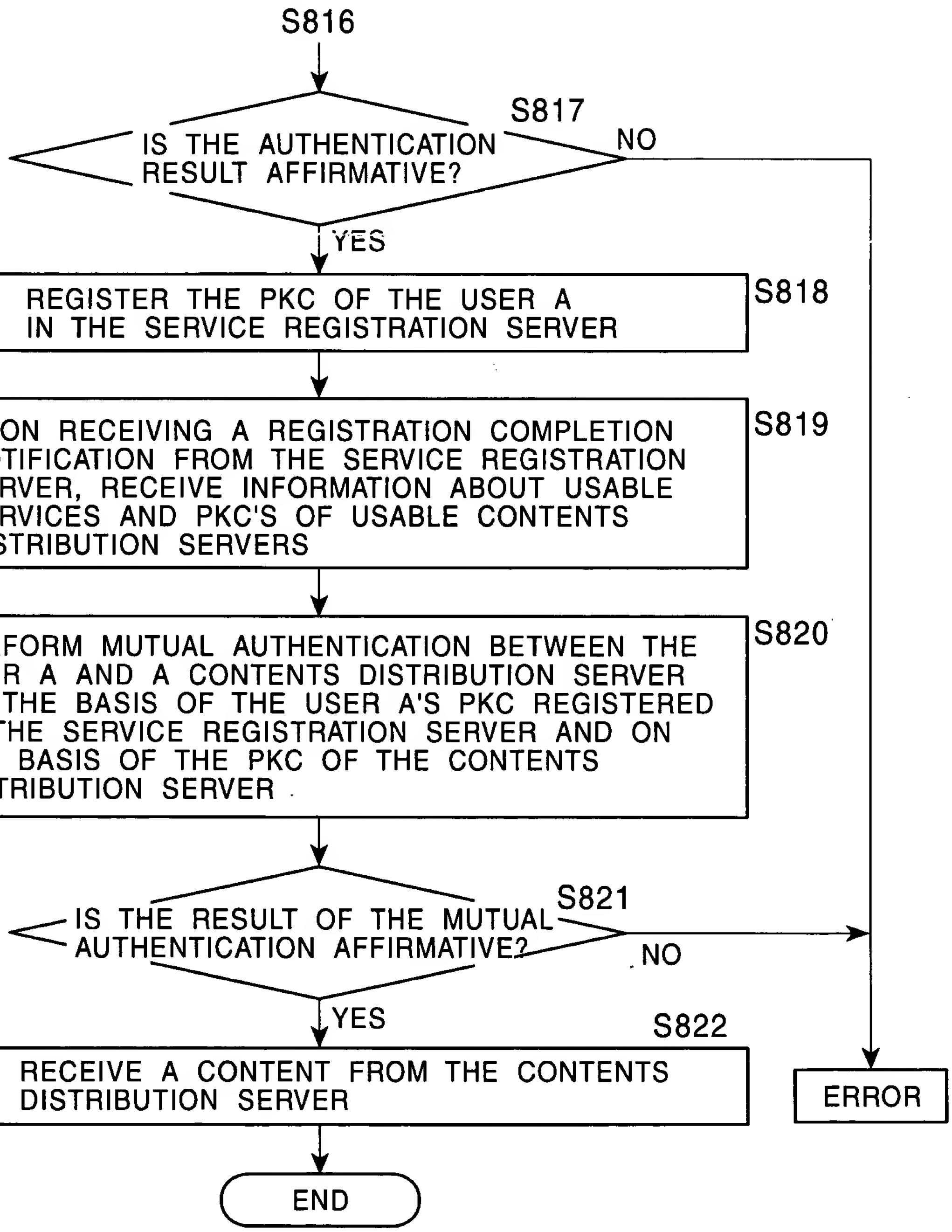

S816
S817
IS THE AUTHENTICATION RESULT AFFIRMATIVE?
NO
YES
REGISTER THE PKC OF THE USER A IN THE SERVICE REGISTRATION SERVER
S818
UPON RECEIVING A REGISTRATION COMPLETION NOTIFICATION FROM THE SERVICE REGISTRATION SERVER, RECEIVE INFORMATION ABOUT USABLE SERVICES AND PKC'S OF USABLE CONTENTS DISTRIBUTION SERVERS
S819
PERFORM MUTUAL AUTHENTICATION BETWEEN THE USER A AND A CONTENTS DISTRIBUTION SERVER ON THE BASIS OF THE USER A'S PKC REGISTERED IN THE SERVICE REGISTRATION SERVER AND ON THE BASIS OF THE PKC OF THE CONTENTS DISTRIBUTION SERVER
S820
S821
IS THE RESULT OF THE MUTUAL AUTHENTICATION AFFIRMATIVE?
NO
YES
S822
RECEIVE A CONTENT FROM THE CONTENTS DISTRIBUTION SERVER
ERROR
END

FIG. 76

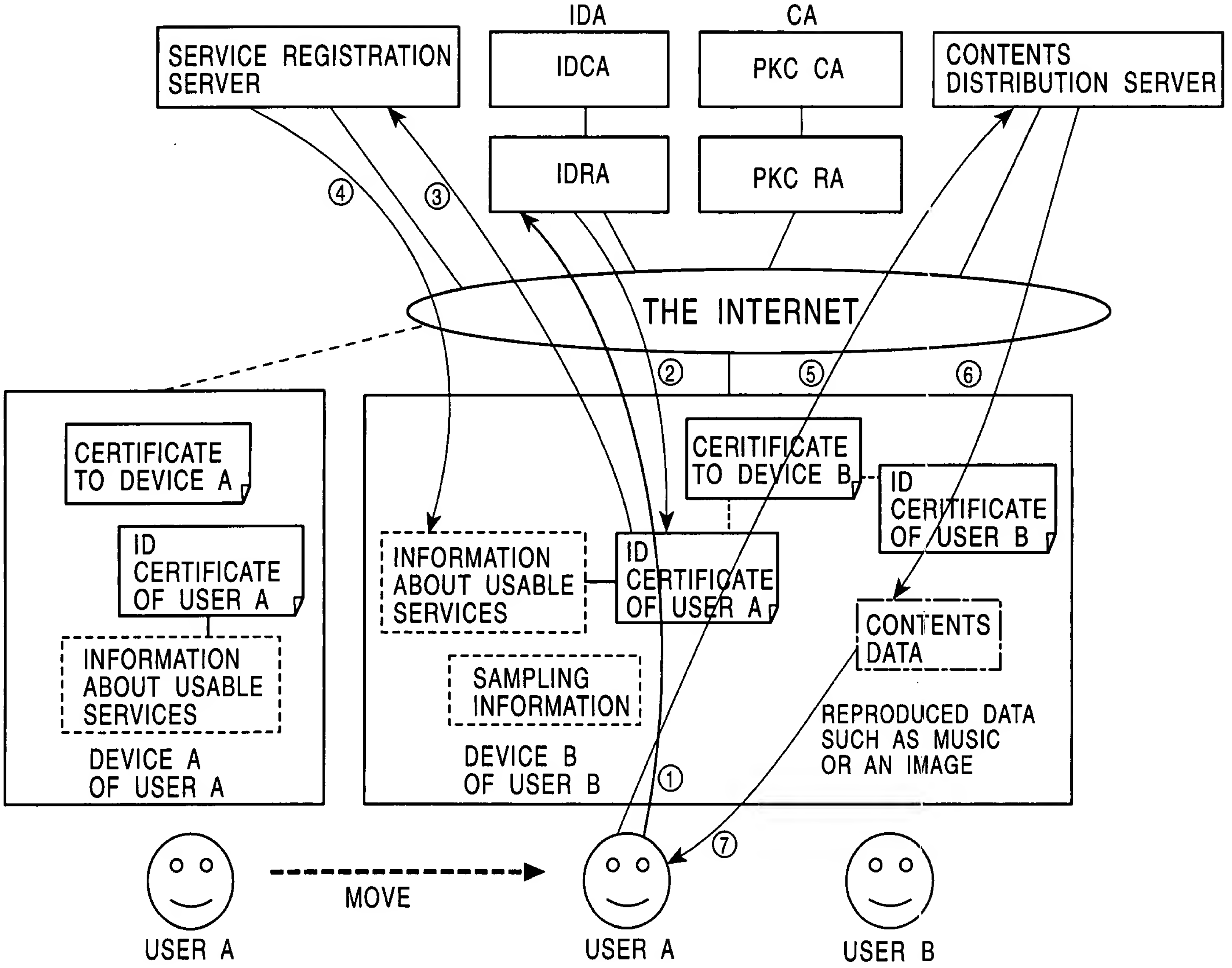

IDA
CA
SERVICE REGISTRATION SERVER
IDCA
PKC CA
CONTENTS DISTRIBUTION SERVER
IDRA
PKC RA
④
③
THE INTERNET
②
⑤
⑥
CERTIFICATE TO DEVICE A
ID CERTIFICATE OF USER A
INFORMATION ABOUT USABLE SERVICES
DEVICE A OF USER A
CERITIFICATE TO DEVICE B
ID CERIFICATE OF USER B
INFORMATION ABOUT USABLE SERVICES
ID CERTIFICATE OF USER A
SAMPLING INFORMATION
CONTENTS DATA
REPRODUCED DATA SUCH AS MUSIC OR AN IMAGE
DEVICE B OF USER B
①
⑦
USER A
MOVE
USER A
USER B

FIG. 77

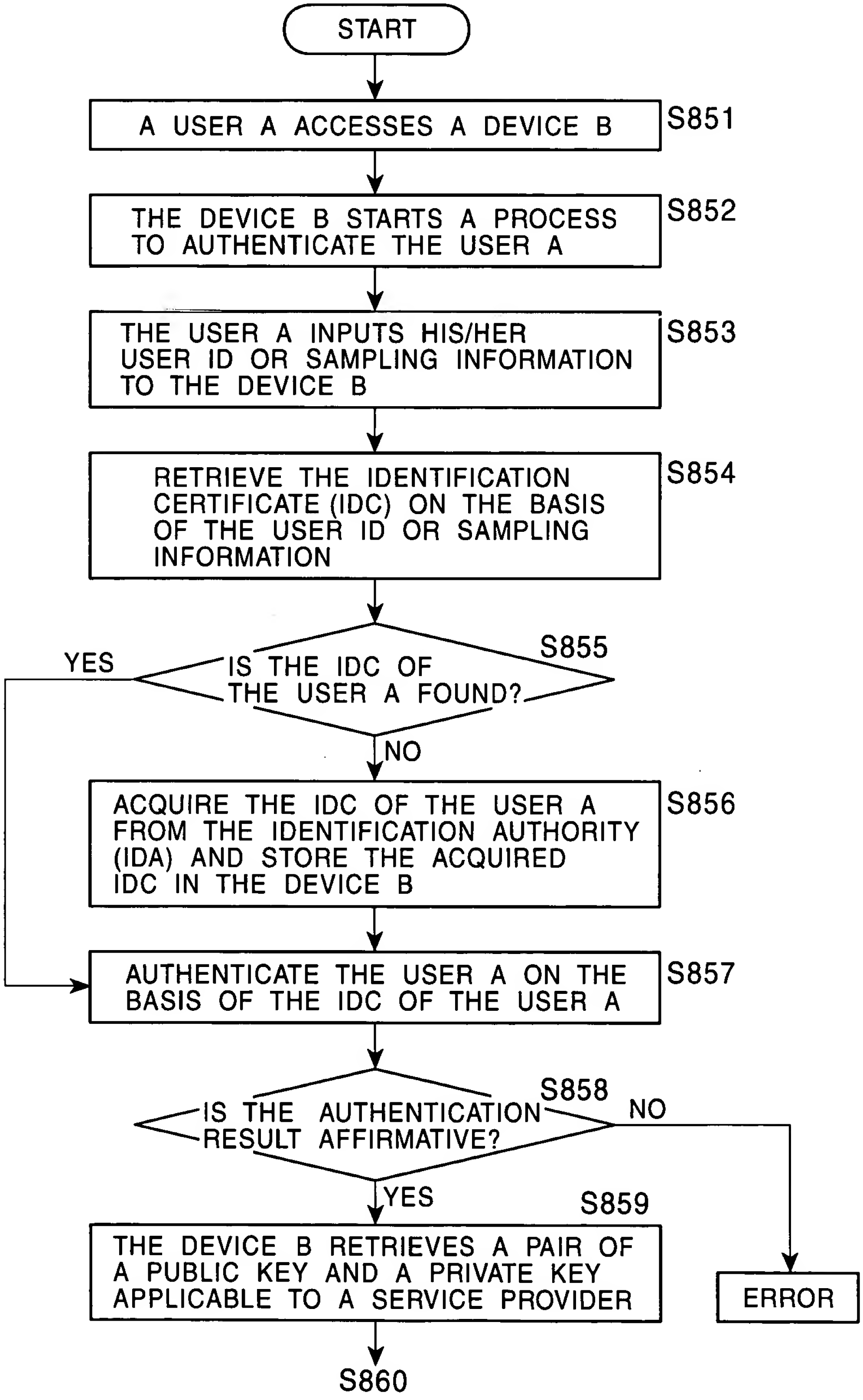

START
A USER A ACCESSES A DEVICE B
S851
THE DEVICE B STARTS A PROCESS TO AUTHENTICATE THE USER A
S852
THE USER A INPUTS HIS/HER USER ID OR SAMPLING INFORMATION TO THE DEVICE B
S853
RETRIEVE THE IDENTIFICATION CERTIFICATE (IDC) ON THE BASIS OF THE USER ID OR SAMPLING INFORMATION
S854
IS THE IDC OF THE USER A FOUND?
S855
YES
NO
ACQUIRE THE IDC OF THE USER A FROM THE IDENTIFICATION AUTHORITY (IDA) AND STORE THE ACQUIRED IDC IN THE DEVICE B
S856
AUTHENTICATE THE USER A ON THE BASIS OF THE IDC OF THE USER A
S857
IS THE AUTHENTICATION RESULT AFFIRMATIVE?
S858
NO
YES
S859
THE DEVICE B RETRIEVES A PAIR OF A PUBLIC KEY AND A PRIVATE KEY APPLICABLE TO A SERVICE PROVIDER
ERROR
S860

FIG. 78

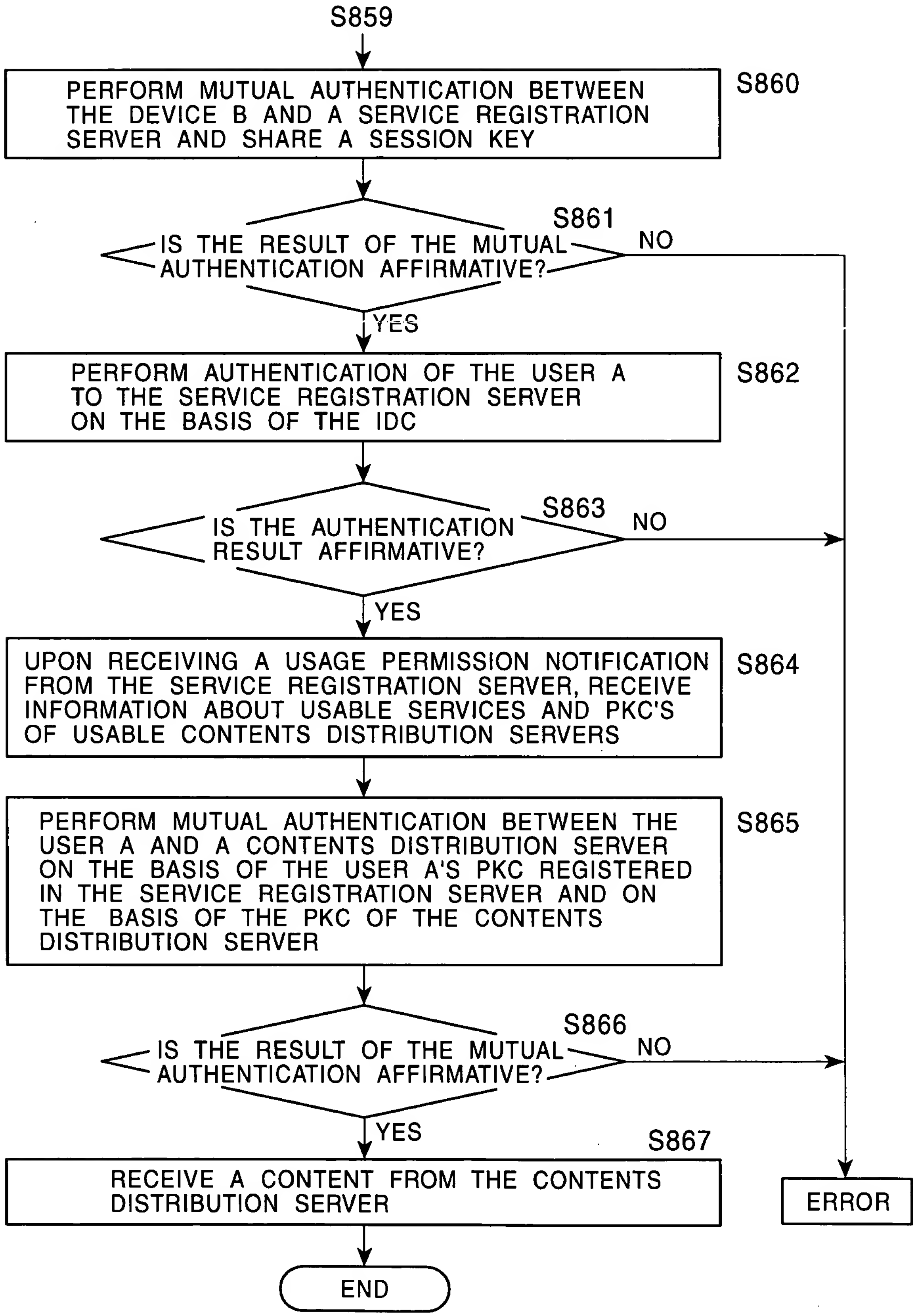

S859
PERFORM MUTUAL AUTHENTICATION BETWEEN THE DEVICE B AND A SERVICE REGISTRATION SERVER AND SHARE A SESSION KEY
S860
S861
IS THE RESULT OF THE MUTUAL AUTHENTICATION AFFIRMATIVE?
NO
YES
PERFORM AUTHENTICATION OF THE USER A TO THE SERVICE REGISTRATION SERVER ON THE BASIS OF THE IDC
S862
S863
IS THE AUTHENTICATION RESULT AFFIRMATIVE?
NO
YES
UPON RECEIVING A USAGE PERMISSION NOTIFICATION FROM THE SERVICE REGISTRATION SERVER, RECEIVE INFORMATION ABOUT USABLE SERVICES AND PKC'S OF USABLE CONTENTS DISTRIBUTION SERVERS
S864
PERFORM MUTUAL AUTHENTICATION BETWEEN THE USER A AND A CONTENTS DISTRIBUTION SERVER ON THE BASIS OF THE USER A'S PKC REGISTERED IN THE SERVICE REGISTRATION SERVER AND ON THE BASIS OF THE PKC OF THE CONTENTS DISTRIBUTION SERVER
S865
S866
IS THE RESULT OF THE MUTUAL AUTHENTICATION AFFIRMATIVE?
NO
YES
S867
RECEIVE A CONTENT FROM THE CONTENTS DISTRIBUTION SERVER
ERROR
END

FIG. 79

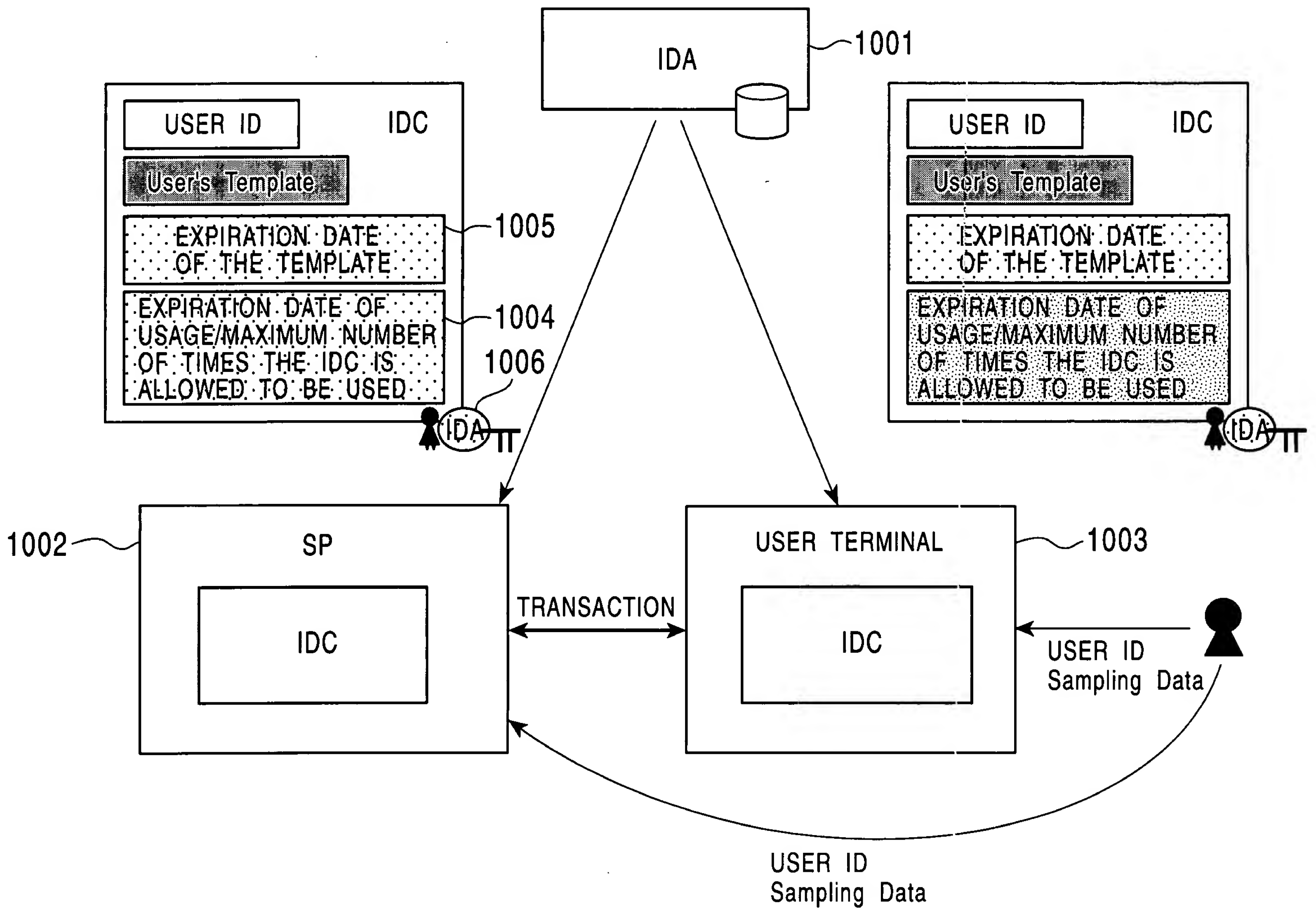

IDA
1001
USER ID
IDC
User's Template
EXPIRATION DATE OF THE TEMPLATE
1005
EXPIRATION DATE OF USAGE/MAXIMUM NUMBER OF TIMES THE IDC IS ALLOWED TO BE USED
1004
1006
IDA
USER ID
IDC
User's Template
EXPIRATION DATE OF THE TEMPLATE
EXPIRATION DATE OF USAGE/MAXIMUM NUMBER OF TIMES THE IDC IS ALLOWED TO BE USED
IDA
1002
SP
IDC
TRANSACTION
USER TERMINAL
IDC
1003
USER ID
Sampling Data
USER ID
Sampling Data

FIG. 80A

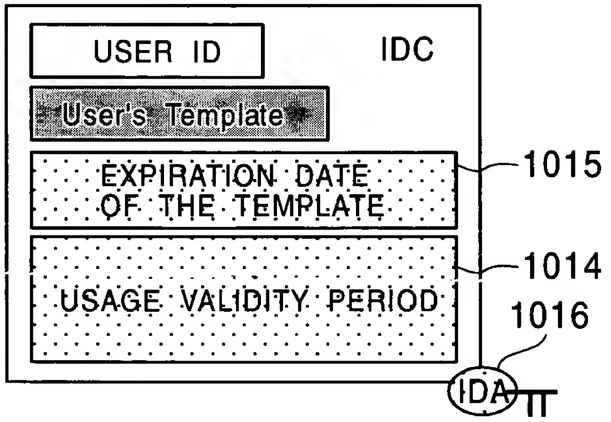


FIG. 80B

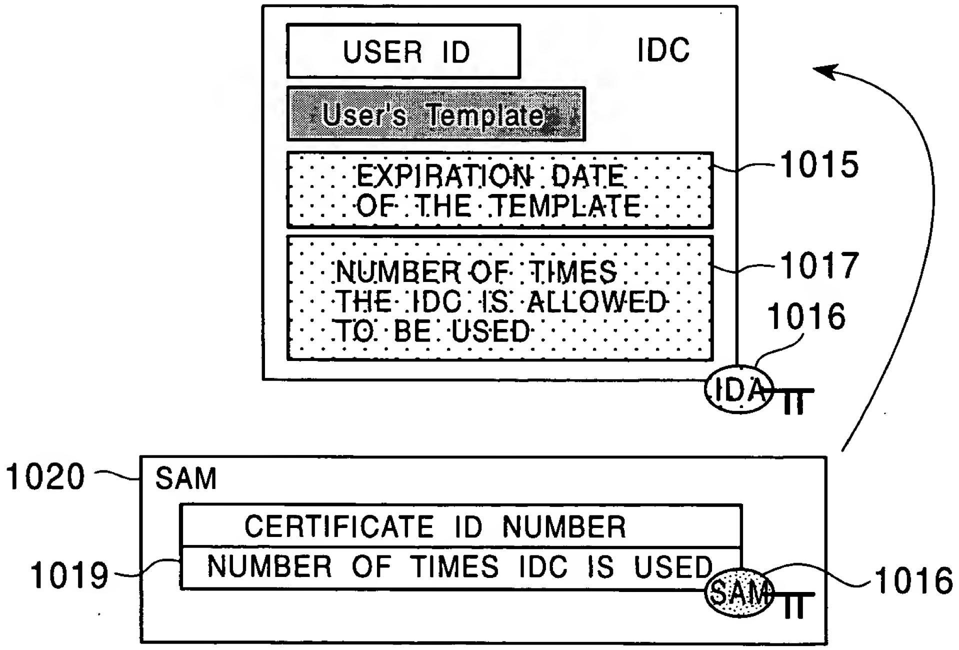

USER ID
IDC
User's Template
EXPIRATION DATE OF THE TEMPLATE
1015
NUMBER OF TIMES THE IDC IS ALLOWED TO BE USED
1017
1016
IDA
1020
SAM
CERTIFICATE ID NUMBER
1019
NUMBER OF TIMES IDC IS USED
SAM
1016

FIG. 81

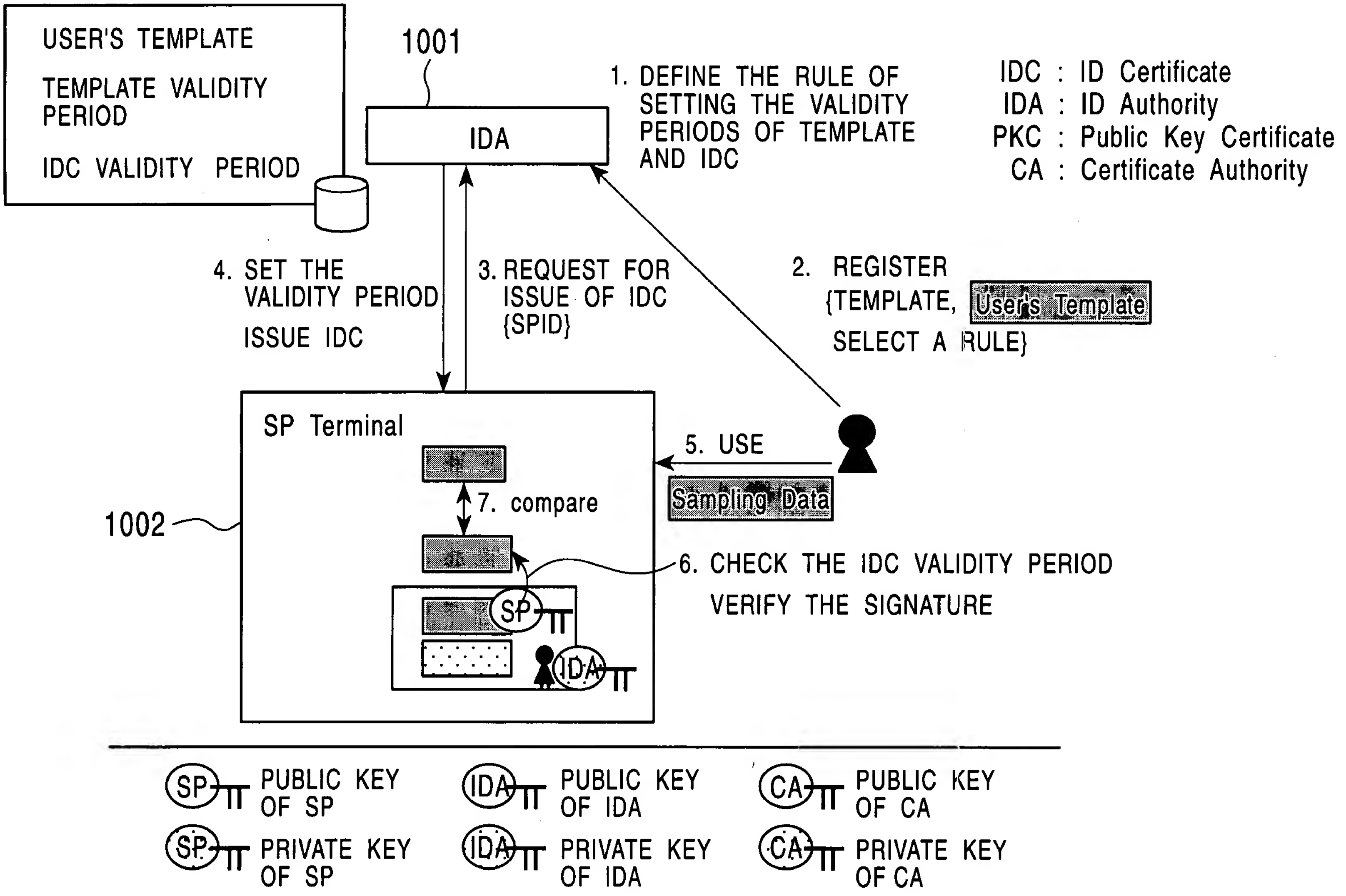

USER'S TEMPLATE
TEMPLATE VALIDITY PERIOD
IDC VALIDITY PERIOD
1001
IDA
1. DEFINE THE RULE OF SETTING THE VALIDITY PERIODS OF TEMPLATE AND IDC
IDC : ID Certificate
IDA : ID Authority
PKC : Public Key Certificate
CA : Certificate Authority
4. SET THE VALIDITY PERIOD
ISSUE IDC
3. REQUEST FOR ISSUE OF IDC {SPID}
2. REGISTER {TEMPLATE, User's Template SELECT A RULE}
SP Terminal
1002
7. compare
5. USE
Sampling Data
6. CHECK THE IDC VALIDITY PERIOD
VERIFY THE SIGNATURE
SP
IDA
SP PUBLIC KEY OF SP
SP PRIVATE KEY OF SP
IDA PUBLIC KEY OF IDA
IDA PRIVATE KEY OF IDA
CA PUBLIC KEY OF CA
CA PRIVATE KEY OF CA

FIG. 82

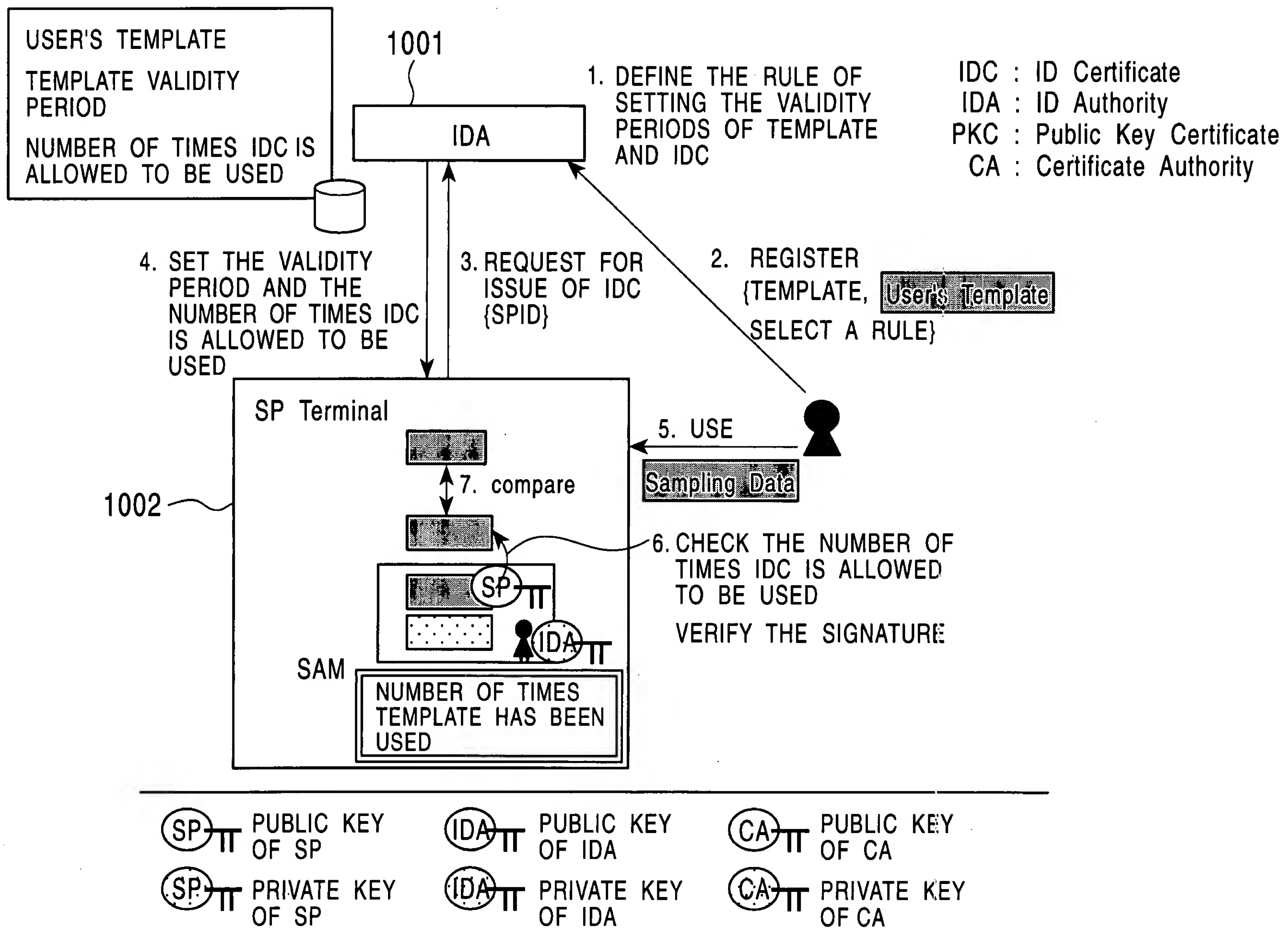

USER'S TEMPLATE
TEMPLATE VALIDITY PERIOD
NUMBER OF TIMES IDC IS ALLOWED TO BE USED
1001
IDA
1. DEFINE THE RULE OF SETTING THE VALIDITY PERIODS OF TEMPLATE AND IDC
IDC : ID Certificate
IDA : ID Authority
PKC : Public Key Certificate
CA : Certificate Authority
2. REGISTER {TEMPLATE, SELECT A RULE}
User's Template
3. REQUEST FOR ISSUE OF IDC {SPID}
4. SET THE VALIDITY PERIOD AND THE NUMBER OF TIMES IDC IS ALLOWED TO BE USED
SP Terminal
1002
5. USE
Sampling Data
7. compare
6. CHECK THE NUMBER OF TIMES IDC IS ALLOWED TO BE USED
VERIFY THE SIGNATURE
SP
IDA
SAM
NUMBER OF TIMES TEMPLATE HAS BEEN USED
SP PUBLIC KEY OF SP
SP PRIVATE KEY OF SP
IDA PUBLIC KEY OF IDA
IDA PRIVATE KEY OF IDA
CA PUBLIC KEY OF CA
CA PRIVATE KEY OF CA

FIG. 83

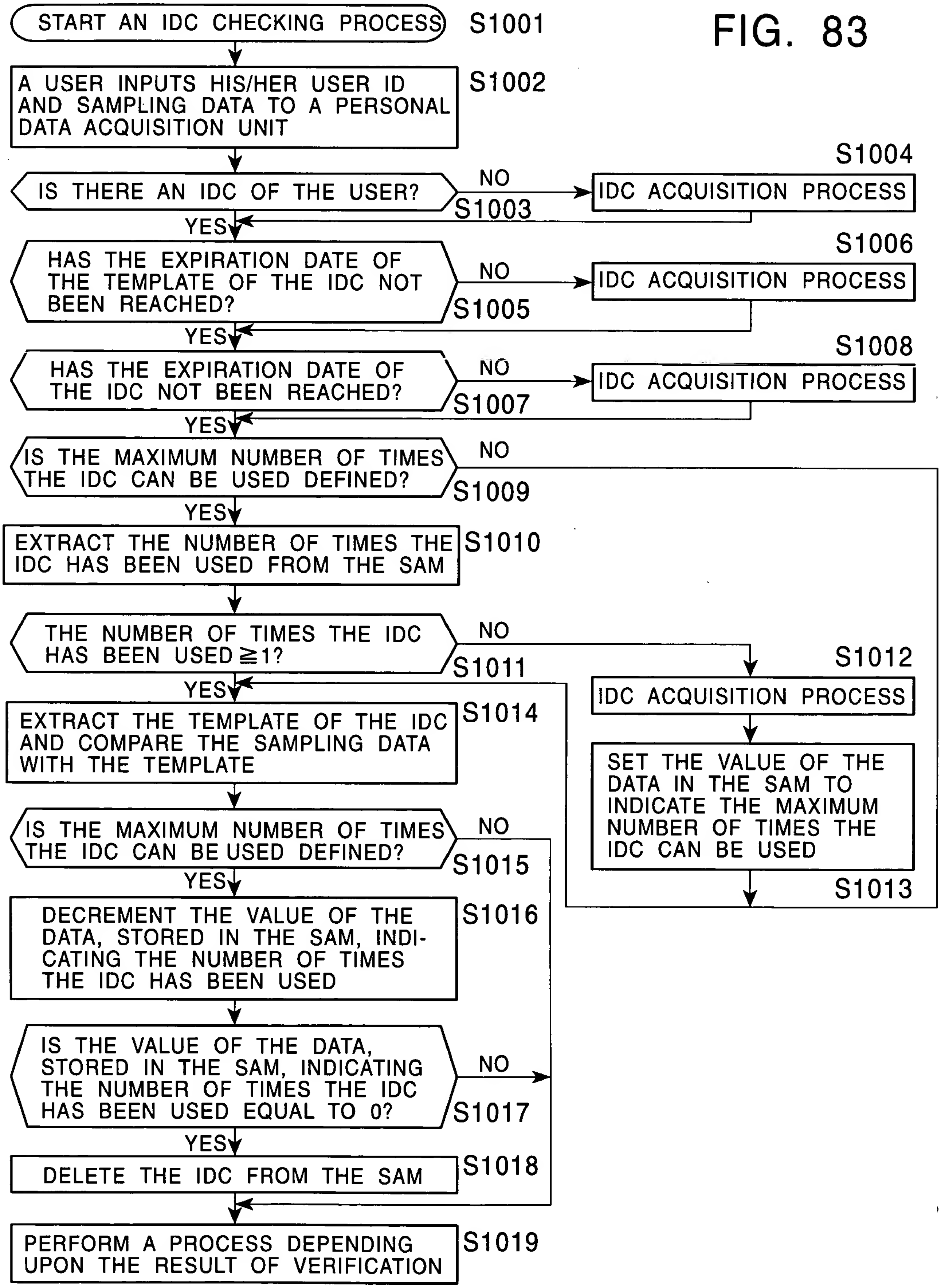
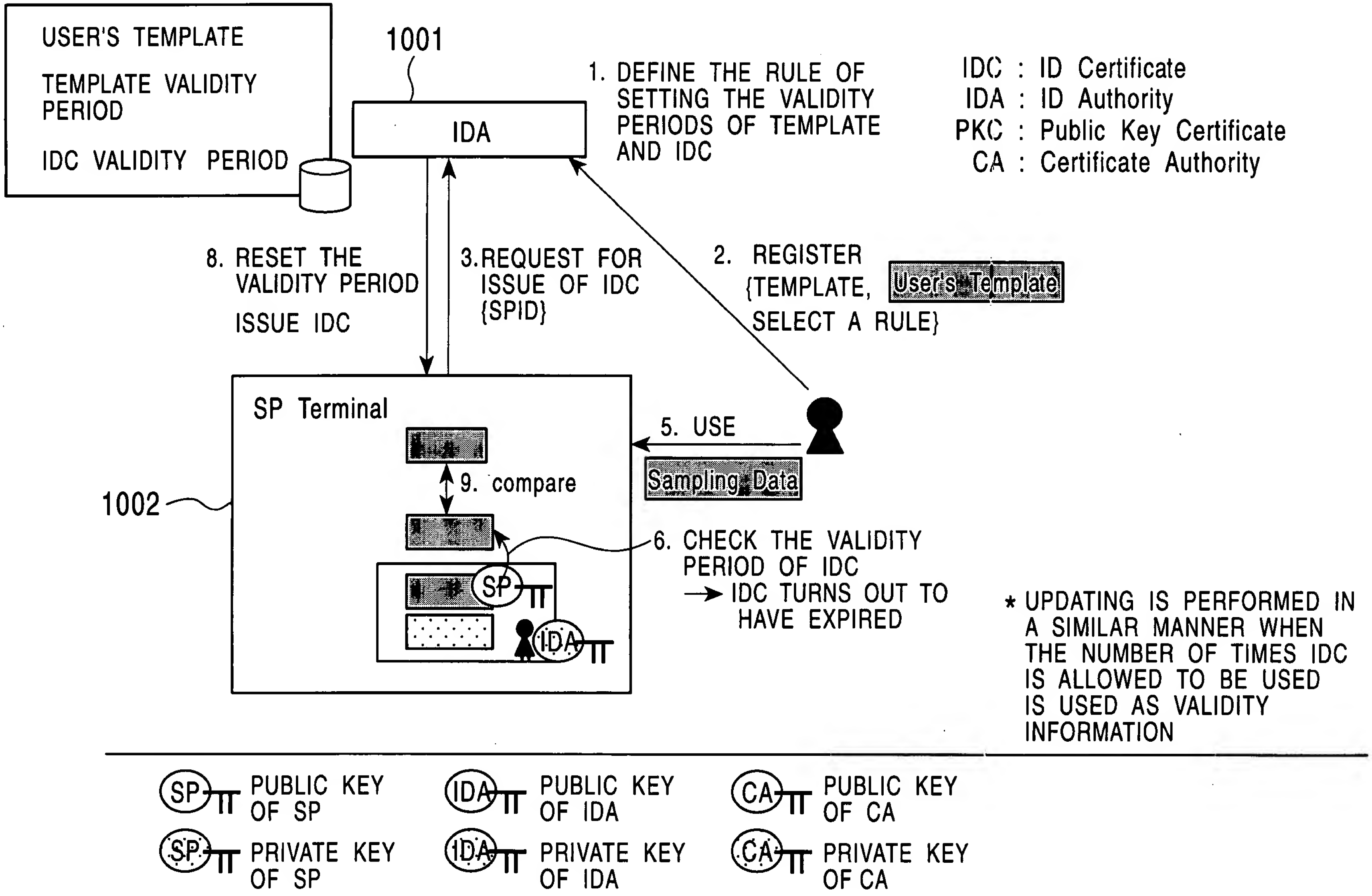

START AN IDC CHECKING PROCESS
S1001
A USER INPUTS HIS/HER USER ID AND SAMPLING DATA TO A PERSONAL DATA ACQUISITION UNIT
S1002
IS THERE AN IDC OF THE USER?
S1003
NO
IDC ACQUISITION PROCESS
S1004
YES
HAS THE EXPIRATION DATE OF THE TEMPLATE OF THE IDC NOT BEEN REACHED?
S1005
NO
IDC ACQUISITION PROCESS
S1006
YES
HAS THE EXPIRATION DATE OF THE IDC NOT BEEN REACHED?
S1007
NO
IDC ACQUISITION PROCESS
S1008
YES
IS THE MAXIMUM NUMBER OF TIMES THE IDC CAN BE USED DEFINED?
S1009
NO
YES
EXTRACT THE NUMBER OF TIMES THE IDC HAS BEEN USED FROM THE SAM
S1010
THE NUMBER OF TIMES THE IDC HAS BEEN USED ≧1?
S1011
NO
IDC ACQUISITION PROCESS
S1012
SET THE VALUE OF THE DATA IN THE SAM TO INDICATE THE MAXIMUM NUMBER OF TIMES THE IDC CAN BE USED
S1013
YES
EXTRACT THE TEMPLATE OF THE IDC AND COMPARE THE SAMPLING DATA WITH THE TEMPLATE
S1014
IS THE MAXIMUM NUMBER OF TIMES THE IDC CAN BE USED DEFINED?
S1015
NO
YES
DECREMENT THE VALUE OF THE DATA, STORED IN THE SAM, INDICATING THE NUMBER OF TIMES THE IDC HAS BEEN USED
S1016
IS THE VALUE OF THE DATA, STORED IN THE SAM, INDICATING THE NUMBER OF TIMES THE IDC HAS BEEN USED EQUAL TO 0?
S1017
NO
YES
DELETE THE IDC FROM THE SAM
S1018
PERFORM A PROCESS DEPENDING UPON THE RESULT OF VERIFICATION
S1019

FIG. 84


USER'S TEMPLATE
TEMPLATE VALIDITY PERIOD
IDC VALIDITY PERIOD
1001
IDA
1. DEFINE THE RULE OF SETTING THE VALIDITY PERIODS OF TEMPLATE AND IDC
2. REGISTER {TEMPLATE, User's Template SELECT A RULE}
3.REQUEST FOR ISSUE OF IDC {SPID}
8. RESET THE VALIDITY PERIOD
ISSUE IDC
1002
SP Terminal
9. compare
SP
IDA
5. USE
Sampling Data
6. CHECK THE VALIDITY PERIOD OF IDC
→ IDC TURNS OUT TO HAVE EXPIRED
SP PUBLIC KEY OF SP
SP PRIVATE KEY OF SP
IDA PUBLIC KEY OF IDA
IDA PRIVATE KEY OF IDA
CA PUBLIC KEY OF CA
CA PRIVATE KEY OF CA

IDC : ID Certificate
IDA : ID Authority
PKC : Public Key Certificate
CA : Certificate Authority

* UPDATING IS PERFORMED IN A SIMILAR MANNER WHEN THE NUMBER OF TIMES IDC IS ALLOWED TO BE USED IS USED AS VALIDITY INFORMATION

FIG. 85

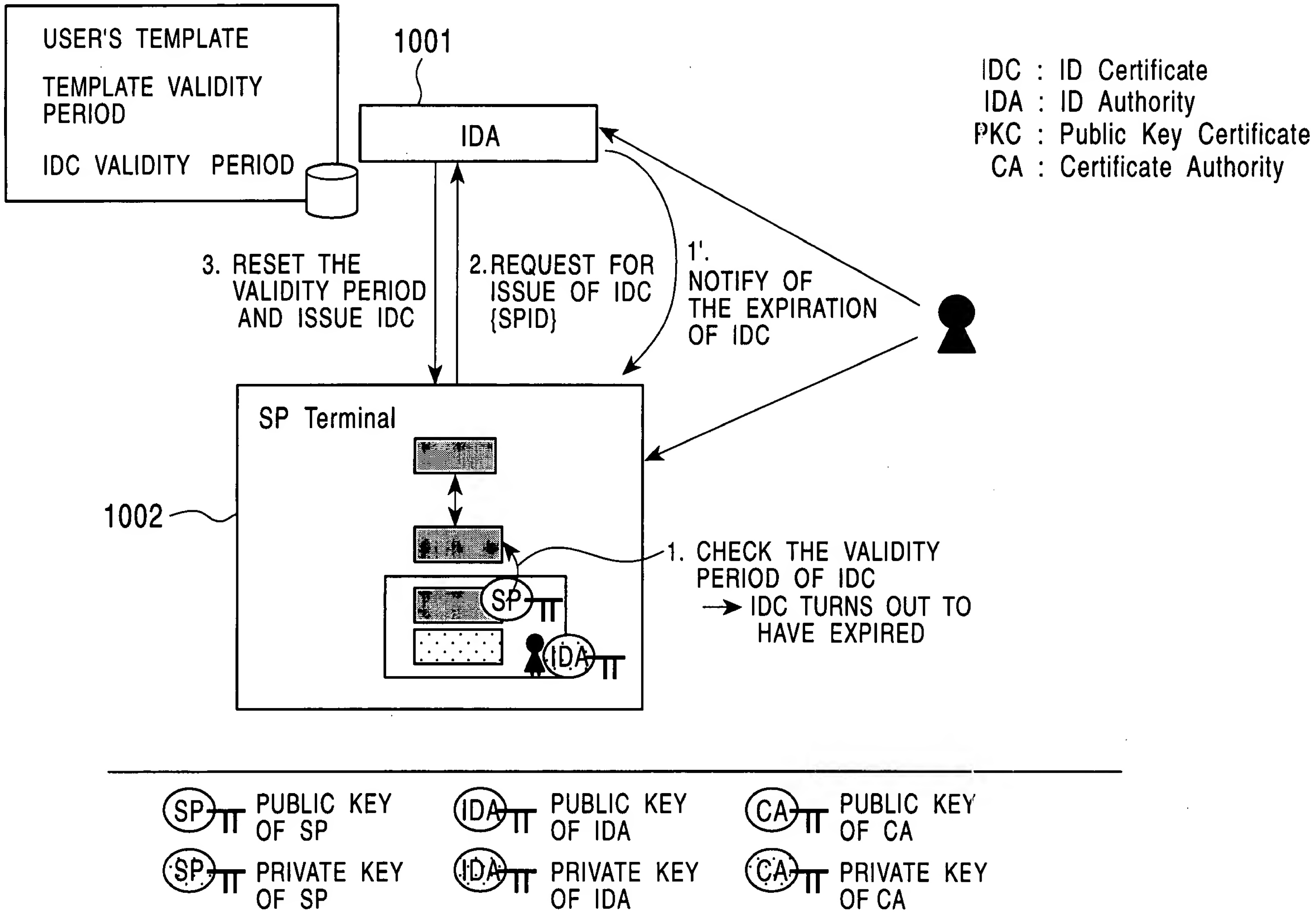

USER'S TEMPLATE
TEMPLATE VALIDITY PERIOD
IDC VALIDITY PERIOD
1001
IDA
IDC : ID Certificate
IDA : ID Authority
PKC : Public Key Certificate
CA : Certificate Authority
3. RESET THE VALIDITY PERIOD AND ISSUE IDC
2. REQUEST FOR ISSUE OF IDC {SPID}
1'. NOTIFY OF THE EXPIRATION OF IDC
SP Terminal
1002
SP
IDA
1. CHECK THE VALIDITY PERIOD OF IDC
→ IDC TURNS OUT TO HAVE EXPIRED
SP PUBLIC KEY OF SP
SP PRIVATE KEY OF SP
IDA PUBLIC KEY OF IDA
IDA PRIVATE KEY OF IDA
CA PUBLIC KEY OF CA
CA PRIVATE KEY OF CA

FIG. 86

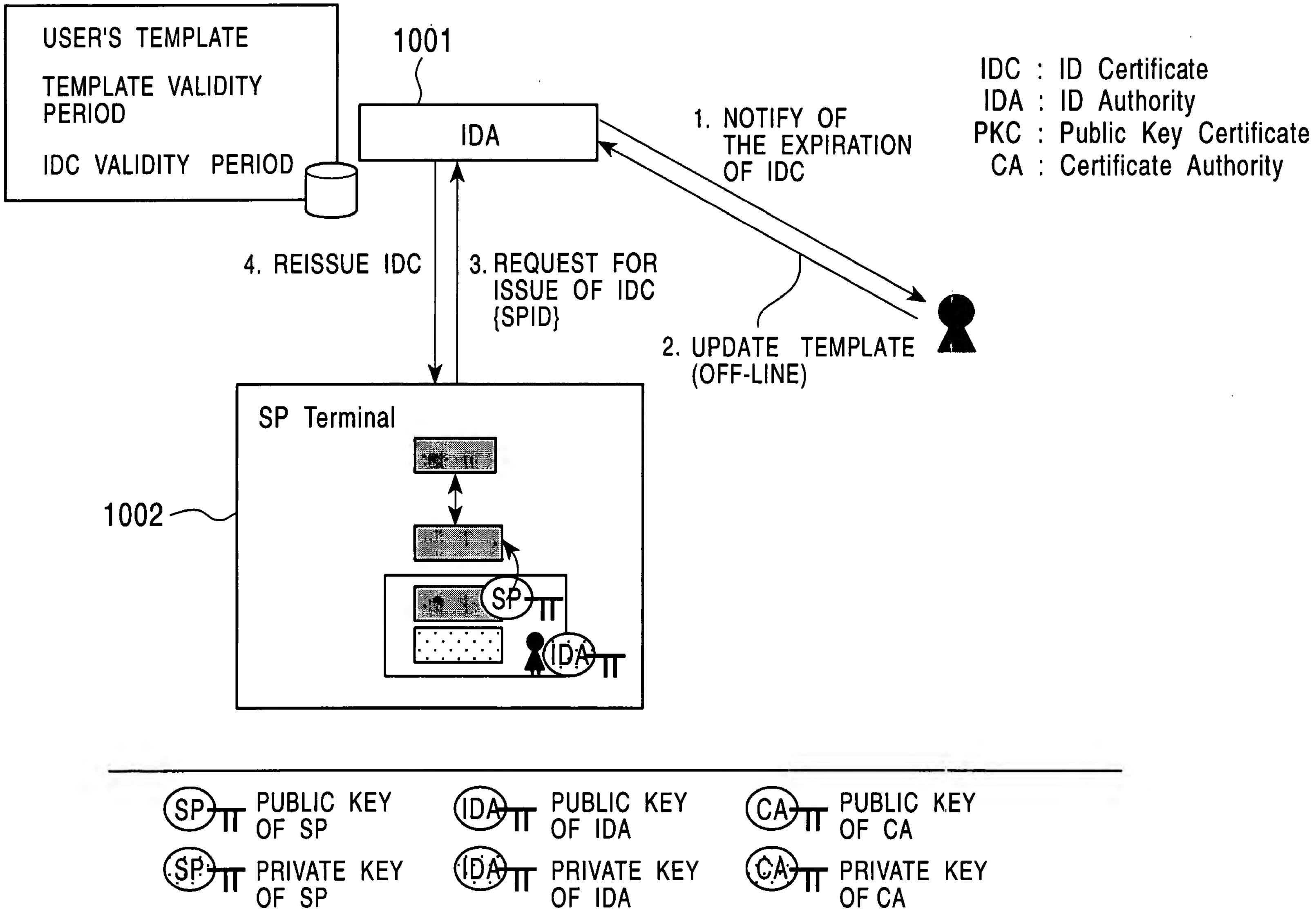
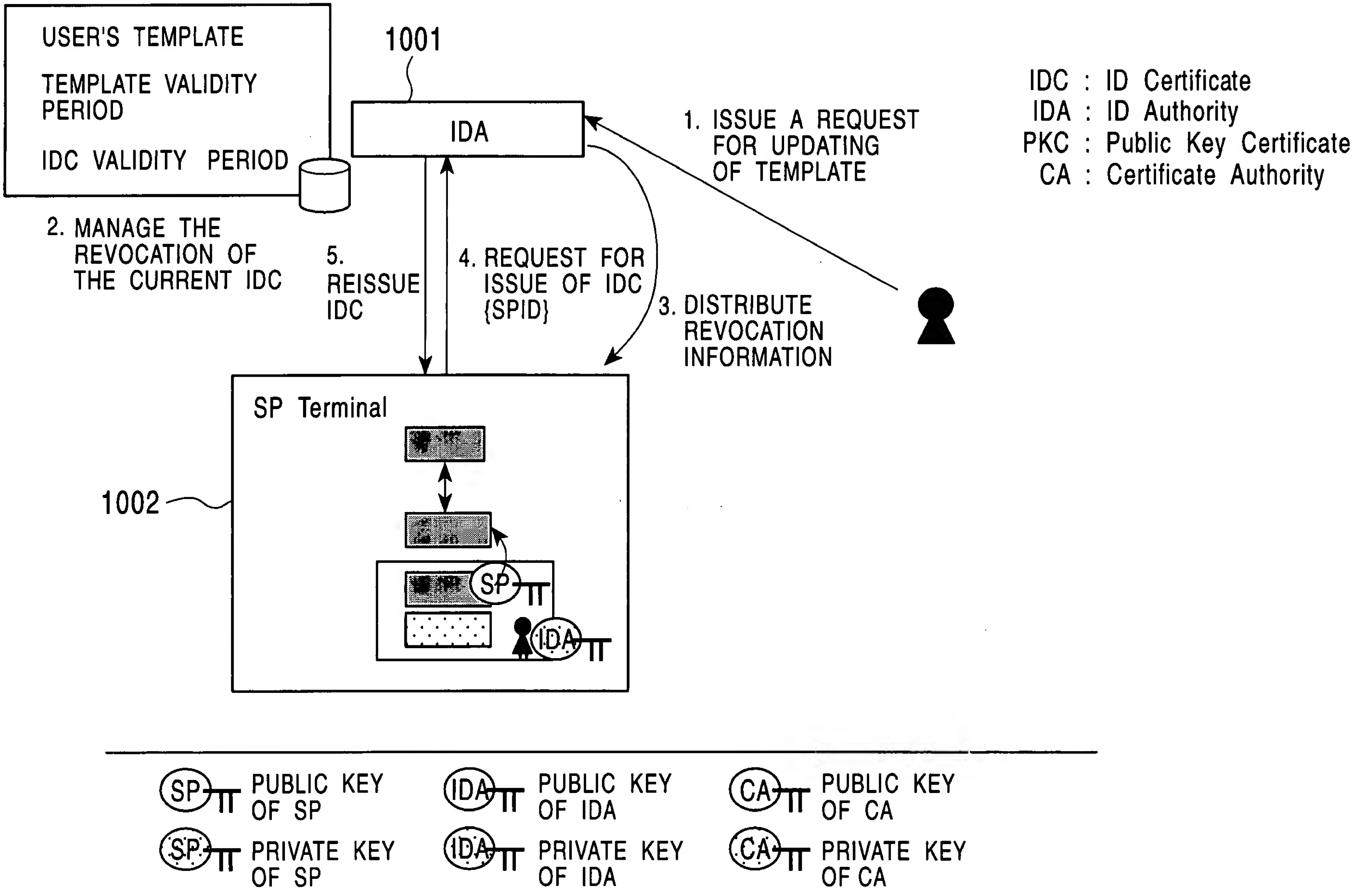

USER'S TEMPLATE
TEMPLATE VALIDITY PERIOD
IDC VALIDITY PERIOD
1001
IDA
1. NOTIFY OF THE EXPIRATION OF IDC
2. UPDATE TEMPLATE (OFF-LINE)
3. REQUEST FOR ISSUE OF IDC {SPID}
4. REISSUE IDC
1002
SP Terminal
SP
IDA
IDC : ID Certificate
IDA : ID Authority
PKC : Public Key Certificate
CA : Certificate Authority
SP PUBLIC KEY OF SP
SP PRIVATE KEY OF SP
IDA PUBLIC KEY OF IDA
IDA PRIVATE KEY OF IDA
CA PUBLIC KEY OF CA
CA PRIVATE KEY OF CA

FIG. 87


USER'S TEMPLATE
TEMPLATE VALIDITY PERIOD
IDC VALIDITY PERIOD
1001
IDA
1. ISSUE A REQUEST FOR UPDATING OF TEMPLATE
2. MANAGE THE REVOCATION OF THE CURRENT IDC
3. DISTRIBUTE REVOCATION INFORMATION
4. REQUEST FOR ISSUE OF IDC {SPID}
5. REISSUE IDC
SP Terminal
1002
SP
IDA
IDC : ID Certificate
IDA : ID Authority
PKC : Public Key Certificate
CA : Certificate Authority
SP PUBLIC KEY OF SP
SP PRIVATE KEY OF SP
IDA PUBLIC KEY OF IDA
IDA PRIVATE KEY OF IDA
CA PUBLIC KEY OF CA
CA PRIVATE KEY OF CA